Gérer les enjeux et risques juridiques du Web 2.0

JANVIER 2012







Le CEFRIO est le centre facilitant la recherche et l'innovation dans les organisations, à l'aide des technologies de l'information et de la communication (TIC). Il regroupe plus de 150 membres universitaires, industriels et gouvernementaux ainsi que 60 chercheurs associés et invités. Sa mission : contribuer à faire du Québec une société numérique, grâce à l'usage des technologies comme levier de l'innovation sociale et organisationnelle. Le CEFRIO, en tant que centre de liaison et de transfert, réalise, en partenariat, des projets de recherche-expérimentation, d'enquêtes et de veille stratégique sur l'appropriation des TIC à l'échelle québécoise et canadienne. Ces projets touchent l'ensemble des secteurs de l'économie, tant privé que public. Les activités du CEFRIO sont financées à près de 64 % par ses propres projets et à 36 % par le ministère du Développement économique, de l'Innovation et de l'Exportation, son principal partenaire financier.



PRINCIPAL PARTENAIRE FINANCIER DU CEFRIO

Gérer les enjeux et risques juridiques du Web 2.0

Le CEFRIO, à travers ce projet d'expérimentation, vise à regrouper des organisations avant-gardistes qui ont un intérêt commun : comprendre, utiliser et tirer profit des nouvelles approches des médias sociaux. L'objectif principal du projet est de susciter l'innovation vers de nouvelles pratiques par l'usage des outils du Web 2.0 et d'en partager les résultats entre les organisations. Pour plus d'information et pour consulter les nouvelles du projet : http://www.cefrio.qc.ca/projet/web_2_0.html

Auteurs – Université de Montréal :
Pierre Trudel
France Abran

Collaborateurs – Université de Montréal :
Julien Fournier
Cynthia Gaudette
Annie Lagueux
Geneviève Normand
Jean-François R. Ouellette

Équipe de projet – CEFRIO
Josée Beaudoin, vice-présidente Montréal, Innovation et Transfert
Julia Gaudreault-Perron, chargée de projet

Graphisme – Ayograph
Brigitte Ayotte

Photos de la couverture
iStockphoto.com : ©STEEX
iStockphoto.com : ©d619

Pour tout renseignement concernant le projet, veuillez communiquer avec le CEFRIO aux coordonnées ci-dessous :

Québec - Siège social 888, rue Saint-Jean Bureau 575 Québec (Québec) G1R 5H6 Canada Téléphone : 418 523-3746 Télécopieur : 418 523-2329	**Montréal** 550, rue Sherbrooke Ouest Bureau 471, Tour Ouest Montréal (Québec) H3A 1B9 Canada Téléphone : 514 840-1245 Télécopieur : 514 840-1275

Courriel : info@cefrio.qc.ca – Site Internet : www.cefrio.qc.ca

Dépôt légal : 2012
Bibliothèques et Archives nationales du Québec
Bibliothèques et Archives Canada
ISBN : 978-2-923852-29-4

Avant-propos

En 2011, 73 % des internautes québécois ont réalisé au moins une activité par mois sur les médias sociaux et près du tiers de ceux-ci y ont déjà suivi une marque, une entreprise, un organisme ou un ministère (31 %). Dans la moitié des cas, ces derniers ont interagi avec l'une ou l'autre de ces organisations sur les médias sociaux.

Dans ce contexte, où une réelle attente de la population est présente, il est difficile pour les organisations québécoises d'ignorer ce moyen de communication privilégié auprès de leur clientèle. Plus encore, le Web 2.0 au sens plus large recèle de réelles opportunités de création de valeur pour l'entreprise de demain, tant à l'interne qu'à l'externe. Plusieurs organisations ont compris l'importance d'explorer ce que représente pour chacune d'elles ce nouveau paradigme, dont celles qui ont choisi de prendre part au projet de recherche-expérimentation du CEFRIO sur les nouveaux usages du Web 2.0.

Constatant l'évolution fulgurante de l'usage du Web 2.0 par la population et, progressivement, des organisations, le CEFRIO a lancé à l'automne de 2009 un vaste chantier sur les nouveaux usages du Web 2.0 pour les organisations. Une douzaine d'organisations ont pris part au projet à titre de partenaires d'expérimentation ou de partenaires financiers : la Banque nationale, la Chaire en éco-conseil de l'UQC, la Commission des normes du travail, Desjardins, Hydro-Québec, Phéromone, la Régie des rentes du Québec, Revenu Québec, Services Québec, la Ville de Montréal/Living Lab de Montréal et la Ville de Québec. Il s'agissait alors de susciter l'innovation vers de nouvelles pratiques par l'usage des outils du Web 2.0 et d'en partager les résultats entre les organisations.

Dans ce vaste projet, deux axes d'expérimentation et, incidemment de recherche, ont été adoptés : d'une part, l'axe du processus marketing et de la relation client et, d'autre part, celui des ressources humaines et de la collaboration interne. Un regard sur les enjeux juridiques des initiatives Web 2.0 dans les organisations est également posé, ce qui donne lieu à un troisième axe de recherche.

Afin de documenter les cas expérimentés dans chacune des organisations et selon son modèle de collaboration avec des équipes de chercheurs universitaires, le CEFRIO a fait appel aux chercheurs suivants :

- Réal Jacob, professeur titulaire au service de l'enseignement du management à HEC Montréal, directeur de la valorisation, du transfert aux entreprises et de la formation des cadres à HEC Montréal et président du comité conseil innovation et transfert du CEFRIO.

- Anne Bourhis, professeure agrégée et directrice du service de l'enseignement de la gestion des ressources humaines à HEC Montréal.

- Sylvain Sénécal, professeur agrégé au service de l'enseignement du marketing à HEC Montréal et titulaire de la Chaire de commerce électronique RBC Groupe financier.

- Pierre Trudel, professeur titulaire au Centre de recherche en droit public (CRDP) de la Faculté de droit de l'Université de Montréal et titulaire de la Chaire L. R. Wilson sur le droit des technologies de l'information et du commerce électronique.

Le présent guide porte sur le volet des enjeux juridiques liés aux usages du Web 2.0 par les organisations.

Introduction

L'utilisation d'Internet permet l'accès à un ensemble sans précédent de services de communication et à des informations de toute nature. Les usagers, les entreprises et les organismes publics découvrent les multiples avantages des applications du Web 2.0.

Mais, sans précautions, les activités d'échange, de recherche et de diffusion d'information sur Internet peuvent comporter des écueils et miner la confiance essentielle à la réalisation d'activités significatives[1]. Ces écueils ne sont pas pires que ceux qui sont associés à bien d'autres activités. En particulier, il y a des risques de se trouver dans une situation pour laquelle la loi a prévu des exigences ou des interdits. Au risque de heurter les valeurs de la vie en société ou de se trouver en situation de contravention aux lois, il importe de savoir identifier de telles situations et de se donner les moyens de reconnaître une situation nécessitant des précautions[2].

L'expression Web 2.0 renvoie à un ensemble de réalités et de situations qui échappent à une définition qui serait exhaustive[3]. Caractérisé par certains éléments emblématiques, le Web 2.0 renvoie à une constellation de fonctions possédant des caractéristiques communes. Parmi ces caractéristiques, il y a un niveau élevé d'implication des usagers dans la création de contenus. On associe également au Web 2.0 ces environnements structurés dans lesquels les contenus sont générés en bonne partie par les utilisateurs comme les sites d'édition collective tel celui de l'encyclopédie *Wikipedia*. Ces sites permettent aux internautes d'éditer et de modifier des contenus à leur guise. Dans d'autres cas de figure, on évoque la possibilité de combiner des applications et des

---

1 Jean-Pierre BENGHOZI, Michèle BERGADAÀ et Erwan BURKHART, Web 2.0 *: Enjeux de confiance*, Bruxelles, De Boeck, 2011, p. X.

2 Certains désignent les enjeux relatifs aux valeurs de la vie en société ou de la contravention aux lois en utilisant le mot « éthique ». Mais, dans la plupart des sociétés démocratiques, la quasi-totalité des enjeux est reflétée dans les exigences des lois adoptées par les législateurs. Ces lois reflètent les valeurs jugées importantes par les sociétés concernées. Il n'est donc pas nécessaire de passer par l'éthique pour rendre compte des enjeux et risques associés aux activités qui peuvent se dérouler dans les environnements du Web 2.0. D'ailleurs, les ouvrages qui se présentent comme portant sur l'éthique dans les environnements numériques abordent les mêmes questions que celles abordées dans les lois, mais de façon moins précise au regard des droits et obligations. Il est approprié de recourir aux raisonnements éthiques dans les situations limites, celles pour lesquelles les lois ne procurent pas de solution certaine. Voir notamment: Charles ESS, *Digital Media Ethics*, Cambridge, Polity Press, 2009; Luciano FLORIDI (ed.) *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, 2010.

3 Dion HINCHCLIFFE, « Review of the Year's Best Web 2.0 Explanations' », *Web 2.0 Journal*, http://web2.sys-con.com/node/165914 ; Pierre TRUDEL, « La régulation du Web 2.0 », (2008) 32 *Revue du droit des technologies de l'information* 283.

contenus et synchroniser un site Web avec d'autres[4]. Les sites de partage de contenus comme YouTube ou *Dailymotion* permettent aux internautes de diffuser des contenus en ligne. Les sites de réseaux sociaux comme *Facebook* ou *Myspace* permettent aux individus de diffuser leur profil personnel de même que des informations portant sur d'autres personnes[5]. Un auteur observe que la notion de Web 2.0 « désigne la tendance, observée chez certaines entreprises présentes sur le Web, à publier un contenu généré par les utilisateurs plutôt que de recourir au modèle d'affaires traditionnel de mise en ligne de contenus médiatiques propriétaires. »[6] On associe souvent au Web 2.0 différentes approches caractérisées par le partage de contenus, de mixage de ceux-ci et leur réutilisation au gré des initiatives des usagers.

Afin de rendre compte du droit relatif au Web 2.0, il faut s'intéresser à la normativité effectivement agissante : celle qui engendre suffisamment de risques auprès des acteurs pour que ceux-ci jugent opportun de s'y conformer[7]. Le droit étatique n'est pas seul à encadrer les activités sur Internet : la normativité qui encadre les ressources associées au Web 2.0 procède de ce que la technique permet ou prohibe, elle résulte en grande partie des pratiques observées par les différents acteurs. Ces configurations et ces pratiques engendrent des risques ou visent à transférer des risques à d'autres. Mais les régulateurs étatiques peuvent estimer que les risques engendrés par des activités se déroulant sur Internet sont suffisamment préoccupants pour imposer aux acteurs des obligations et ainsi baliser ce qu'ils peuvent faire en ligne. Par leur réglementation, ils créent des risques pour les acteurs concernés.

Dans les lignes qui suivent, on précise les objectifs, les destinataires, la portée ainsi que la trame générale de la démarche proposée dans le présent guide.

L'objectif du guide

Ce guide vise à accompagner les individus et les organisations concernés par l'utilisation des applications associées au Web 2.0 afin d'assurer que leurs activités se déroulent dans le respect des lois applicables au Québec.

---

4 Mary MADDEN et Susannah FOX, « Riding the Waves of 'Web 2.0' more than a Buzzword, but still not easily defined, Pew Internet, Backgrounder, http://www.pewinternet.org/Reports/2006/Riding-the-Waves-of-Web-20/Riding-the-Waves/Backgrounder.aspx ; Lis VEASMAN, « 'Piggy Backing' on the Web 2.0 Internet : Copyright Liability and Web 2.0 Mashups », [2008] 30 *COMM/ENT* 311-337.

5 Steven JAMES, « Social Networking Sites: Regulating the Online 'Wild West' of Web 2.0 », [2008] 2 *Ent. L.R.* 47-50.

6 Nicolas W. VERMEYS, « Responsabilité civile et Web 2.0 », *Repères*, juillet 2007, http://rejb.editionsyvonblais.com (page visitée le 27 novembre 2011).

7 Pierre TRUDEL, « La régulation du Web 2.0 », [2008] 32 *Revue du droit des technologies de l'information* 283-307.

À quoi sert ce guide ?

Ce guide explicite les préoccupations relatives à la conduite des personnes dans les environnements du Web 2.0. Il précise les exigences et les précautions à prendre dans le développement et l'exploitation de tels environnements. Il propose une méthode afin de cerner les enjeux et de gérer les risques. Il indique comment identifier les caractéristiques des services de même que les activités pouvant nécessiter des mesures et précautions spécifiques. Il procure des aides afin d'identifier les risques et de mettre en place les précautions nécessaires pour que les environnements du Web 2.0 fonctionnent en conformité avec les valeurs et les lois applicables au Québec. Il procure un outil afin d'aider les différents acteurs du Web 2.0 à aligner leurs comportements sur les exigences découlant des lois applicables et des autres normativités pertinentes sur Internet.

À qui est-il destiné ?

Ce guide est destiné principalement aux personnes responsables de la mise en place de politiques et de lignes de conduite relatives et à la gestion ou à l'utilisation de sites ou environnements possédant les caractéristiques du Web 2.0. Il sera également utile aux usagers des divers environnements d'Internet. Il fournit des informations sur les risques à gérer et les précautions à prendre par tous ceux qui œuvrent à la conception, au développement, à l'implantation et à l'usage de systèmes d'information destinés à soutenir des échanges entre les personnes.

Quelle est la portée de ce guide ?

Bien que les questions relatives aux risques et aux enjeux juridiques se posent en une multitude de situations dans le monde virtuel ou ailleurs, le présent guide traite principalement des risques les plus courants dans le cadre des échanges prenant place dans des environnements à contenu entièrement ou partiellement généré par l'utilisateur. Bien que l'on ait mis beaucoup de soins à identifier les dispositions des lois qui trouvent application dans les situations les plus courantes, ce guide ne constitue pas un avis juridique. Les conseils qu'il comporte sont de portée générale et ne sauraient remplacer une expertise spécifique dans des cas particuliers.

Dans ce guide, l'on aborde les dimensions juridiques du Web 2.0 selon une approche de gestion de risques. Le respect des lois n'est pas, en soi, une question de degré : on doit toujours respecter les lois. Mais souvent, lorsqu'on met en place des activités se déroulant sur Internet, on trouve opportun de prévoir les difficultés juridiques susceptibles de découler des activités que l'on propose, permet ou accueille, en évaluant les risques que s'appliquent effectivement des règles susceptibles d'engendrer un effet non souhaité.

L'approche proposée ici relève d'une démarche par laquelle on analyse les environnements, les activités de même que les caractéristiques des personnes

concernées afin de prendre les mesures préventives qui réduiront les risques de se trouver en contravention avec les lois.

La démarche proposée

Elle se présente en quatre temps :

1. **Situer les responsabilités** : identifier qui fait quoi et qui répond de ce qui se passe lors d'une activité se déroulant sur Internet.
2. **Identifier les risques** : pour cela, il faut partir des activités se déroulant sur Internet sous les auspices de l'entreprise ou de l'organisme.
3. **Évaluer les risques** : une telle évaluation tient compte aussi bien des caractéristiques de l'activité que du fonctionnement ou de la configuration des outils Internet utilisés.
4. Enfin, **identifier et mettre en place les mesures et politiques** qui permettent une prise en charge appropriée des risques.

L'approche générale

Chacun des utilisateurs d'Internet doit se familiariser avec les façons de faire compatibles avec le respect des droits des autres. L'on convient de plus en plus qu'il est futile de tenter d'interdire l'accès aux divers environnements en ligne. Il est plus utile de former chacun des usagers à la gestion des risques inhérents aux environnements d'Internet puisque les usagers sont plus que jamais en situation de poser des gestes qui peuvent engendrer des conséquences.

Dans un environnement où l'usager dispose de tant de capacité de transmettre et de recevoir des informations, il est insuffisant de décréter des « conditions d'utilisation » et se réserver simplement le droit de surveiller et de punir. Il est tout aussi contreproductif de multiplier les conditions, contrôles, précautions et processus bureaucratiques sous prétexte d'assurer un environnement protecteur. Sur Internet, le phénomène de la concurrence des régulations joue à plein : les usagers ont plusieurs possibilités de contourner les règles ne répondant pas aux besoins ou formulées de manière irrationnelle.

Si les conditions d'utilisation d'un environnement informatique sont perçues comme trop lourdes où autrement inadaptées aux besoins des acteurs en première ligne, ces derniers ont à leur disposition des services, le plus souvent gratuits et conviviaux, capables de procurer les services ou fonctionnalités recherchées. Mais cela se fait à des conditions qui ne sont pas toujours compatibles avec les exigences qui prévalent ici. Par exemple, si les exigences afin de mettre en place des services de courriel sont mal adaptées ou perçues comme trop lourdes, le risque est grand que les usagers utilisent des outils proposés par les entreprises comme Hotmail ou Yahoo !. Ces outils pourraient ne pas offrir les garanties requises par les lois québécoises.

Sur Internet, plusieurs choix et possibilités d'action sont sous la maîtrise des individus. Il faut donc les informer adéquatement. Il y a des choses qui se règlent plus efficacement au niveau des acteurs directement concernés. C'est pour cette raison que ce guide identifie les responsabilités de chacun des principaux acteurs. Il propose des outils à l'intention de chacun afin de l'aider à décider des mesures à prendre pour gérer les risques qui sont associés à l'une ou l'autre des activités envisagées.

Le fonctionnement de la démarche proposée dans le présent guide se décline en quatre temps qui sont :

> ***Identifier les caractéristiques de l'outil***
>
> *Le Web 2.0 n'est pas un environnement univoque : plusieurs fonctions et services existent et ne présentent pas les mêmes enjeux. Sur Internet, on peut échanger des messages de courriel entre intimes ou diffuser une chanson à la grandeur du réseau. Les risques doivent donc être appréciés à la lumière des caractéristiques que présentent les différents outils disponibles dans le cyberespace.*
>
> ***Identifier les caractéristiques des participants***
>
> *Les décisions à l'égard des politiques et lignes de conduite doivent tenir compte des besoins des destinataires, en fonction de leur position au sein d'une organisation. Les règles doivent être exprimées dans un langage adapté aux usagers concernés.*
>
> ***Identifier les caractéristiques des activités, événements prévus et possibles***
>
> *Toutes les activités ne soulèvent pas les mêmes enjeux. Certaines sont anodines et ne posent pas de problèmes particuliers alors que d'autres nécessitent de plus grandes précautions.*
>
> ***Choisir les politiques et instruments afin de gérer adéquatement les risques***
>
> *Après avoir complété les grilles de questions proposées, le décideur devrait être en mesure de cerner les problématiques qui devront être traitées par ses politiques. Par exemple, sera-t-il nécessaire d'avoir des dispositions sur la conduite à tenir à l'égard du respect du droit d'auteur ? Si oui, quelles sont ces conduites ?*

Les clés de lecture et d'utilisation du guide

Ce guide a été conçu de manière à répondre aux besoins diversifiés de ceux qui ont à prendre des décisions et exercent des responsabilités à l'égard de la mise en place, de la supervision et de la surveillance d'activités prenant place dans des environnements du Web 2.0. Il peut être consulté dans l'ordre de présentation des chapitres. Mais il est possible d'aller directement aux chapitres traitant des questions pour lesquelles on recherche des éclairages.

Si vous cherchez à identifier et à situer les responsabilités que vous avez au sujet de la mise en place, de la surveillance d'activités sur Internet, allez au chapitre II.

Si vous voulez cerner les risques associés aux diverses applications du Web 2.0, allez au chapitre III.

Si vous cherchez des modèles de politiques ou de directives afin d'aider à gérer les risques généraux ou spécifiques à certaines activités, consultez le chapitre IV.

I- Les risques et enjeux découlant des fonctions associées au Web 2.0

Le Web 2.0 n'est peut-être pas complètement nouveau mais il paraît poser, de façon plus dramatique, les enjeux et risques inhérents aux environnements en ligne. Si les risques qu'il implique ne sont pas nécessairement nouveaux, ils paraissent démultipliés. Le rôle accru de l'usager contribue à déplacer et à accroître les lieux où se manifestent des risques et enjeux dont plusieurs peuvent présenter des dimensions juridiques. En raison du rôle actif qu'il tient, l'usager lui-même possède une importante capacité d'engendrer des risques pour les autres.

A. Le changement de l'échelle des risques

Plus que dans l'Internet de première génération, les décisions que prend l'usager sont, susceptibles d'emporter des conséquences pour les tiers. Mais comme l'environnement du Web 2.0 s'inscrit en dehors d'un modèle dans lequel une entité centrale assume les responsabilités, le cadre juridique se présente comme un ensemble de risques répartis entre un nombre indéterminé d'acteurs de dimensions et de statuts différents.

Les risques ont aussi une échelle modifiée en raison des mutations quantitatives et qualitatives de la diffusion de l'information. Internet banalise la circulation de l'information : celle-ci peut aisément se trouver à être diffusée en dehors des cercles de circulation légitime ; d'où l'accroissement des risques.[8] Les environnements du Web 2.0 contribuent à modifier les repères spatiaux et temporels qui permettent de délimiter les lieux de circulation légitime ou licite de l'information. Les multiples fonctions du Web 2.0 donnent accès à des informations qui étaient, il y a peu de temps, tenues pour n'avoir vocation à circuler que dans des espaces restreints. Les balises conçues dans un monde dans lequel les réseaux prenaient moins de place sont prises en défaut[9].

Internet modifie l'échelle spatiale à partir de laquelle s'apprécient les risques. En dehors du monde en réseaux, l'accessibilité à une information exige des ressources qui peuvent être importantes. Sur Internet, on a l'impression que beaucoup d'informations sont à portée d'une requête de moteur de recherche[10]. Une telle facilité d'accès tend à banaliser l'information et accentue les risques de décontextualisation.

---

8 Karl D. BELGUM, « Who leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy [1999] 6 *Rich. J.L. & Tech*. 1.

9 Frederick SCHAUER, « Internet Privacy and the Public-Private Distinction », [1998] 38 *Jurimetrics* 555 ;

10 Daniel J. SOLOVE, « Access and Aggregation : Public Records, Privacy and the Constitution, » [2002] 86 *Minn. L. Rev.,* 1137-1218, p. 1139.

Il y a aussi décentrage temporel : la persistance de l'information entraine le fait que celle-ci traverse les espaces temporels dans lesquels elle était tenue pour légitime. Par exemple, une information peut être légitimement disponible au public en raison de l'actualité de l'événement. L'archivage et la disponibilité virtuellement permanente sur Internet lui confèrent une persistance allant au-delà de ce qui est nécessaire afin de rendre compte de l'actualité.

Les capacités d'agglomération d'information permettent la constitution de gisements d'informations sur les personnes qui peuvent devenir disponibles pour des forces de police de même que constituer des enjeux pour des malfaiteurs. En somme, l'effacement des efforts à consacrer pour trouver l'information occasionne la disparition d'une protection par défaut pour plusieurs droits fondamentaux comme la réputation et la vie privée.

B. Les principales catégories de risques et enjeux

Bien qu'il paraisse impossible d'énumérer, dans l'abstrait, l'ensemble des enjeux et risques que peut poser l'exploitation d'un site Web possédant les caractéristiques associées au Web 2.0, il est possible d'identifier les principales catégories d'enjeux et de risques que la plupart des acteurs voudront considérer afin de calibrer leurs décisions. De façon générique, il est possible de reconnaître que les environnements de Web 2.0 impliquent des risques de comportement, des risques du fait de leur configuration technique ou ergonomique, et des risques de régulation. Chacun de ces risques peut être géré en créant, en transférant ou en accentuant les risques associés à l'une ou l'autre de ces catégories.

1. Les risques de comportement

Il s'agit des risques découlant des comportements que peuvent adopter les internautes qui interagissent sur un site. Les pratiques qui sont susceptibles de mettre à mal les droits des personnes sont celles qui viennent le plus souvent à l'esprit.

Risques pour la réputation des personnes - Avec le Web 2.0, il est facile de parler de soi et des autres et de conférer à de tels propos une diffusion pratiquement universelle. Or, les mécanismes qui assurent la protection du droit à la réputation des personnes tiennent en compte le contexte de la diffusion du propos et apprécient son caractère diffamatoire par rapport au sens qui est donné au propos, compte tenu de l'ensemble des circonstances de sa diffusion. C'est ainsi que l'on peut trouver licite un commentaire formulé en cercle restreint sur les faits et gestes d'une personne dans le cadre de l'exercice de ses fonctions. Mais le même commentaire porté à l'attention d'un tiers non concerné pourra avoir un caractère diffamatoire. Plusieurs environnements associés au Web 2.0 comme les sites de réseautage sociaux procurent des facilités sans précédent de faire passer un propos de l'univers de l'intime à celui du public.

Risques pour la vie privée - Plusieurs applications du Web 2.0 ont le potentiel de briser les lignes séparatrices entre ce qui est tenu pour être privé ou partagé uniquement dans un cercle limité et les informations disponibles à un plus large public. Par exemple, dans un site de réseautage social, il est possible de publier des renseignements nous concernant, mais aussi des renseignements concernant nos contacts. De telles informations peuvent être dévoilées lors de la rédaction d'un commentaire. Nos contacts peuvent également mettre des renseignements nous concernant dans leurs propres sites personnels.

L'accumulation et l'agglomération de données sur les personnes par les sites à contenu généré par les usagers et d'autres fonctions disponibles sur Internet emporte la constitution de répertoires importants d'information potentiellement disponibles aux activités de surveillance de toutes sortes. C'est un risque qui paraît inhérent aux modes de fonctionnement actuel d'Internet.

Risques pour le droit à l'image - Les enjeux relatifs à la diffusion des images mettent en jeu le droit des personnes de s'opposer à la diffusion de leur image sans leur consentement ou en dehors de circonstances où la diffusion serait justifiée par l'intérêt public ou par l'intérêt que pourraient avoir certains proches.

Risques pour la propriété intellectuelle - La banalisation des applications permettant aux usagers de publier des contenus sur des sites Web présente des risques au regard de la propriété intellectuelle : des usagers peuvent reproduire une œuvre sans autorisation puis la publier sans autorisation sur un site. Les principes juridiques de la propriété intellectuelle qui sont interpelés par ce type d'activités ne sont pas nouveaux, mais l'ampleur du phénomène et la facilité avec laquelle il est désormais possible de diffuser des contenus posent des défis majeurs. Les risques de non-conformité aux droits de propriété intellectuelle paraissent accrus[11].

Risques de diffusion de contenus contraires aux lois - Plus on multiplie les lieux de décision en matière de publication sur le réseau, plus les risques de publication de contenus contraires aux lois s'accroissent.

Dans un contexte de site à contenu généré par les usagers, l'ensemble de ces risques découlent principalement des comportements adoptés par les internautes. On se retrouve donc avec une multitude de centres de décision tous en mesure de diffuser des informations à partir de leurs perspectives. Ce rôle accru de l'amateur dans des situations autrefois dominées par des professionnels tend à brouiller les frontières entre

---

11 Jean-Philippe MIKUS et Sébastien ROY, *Choisir et protéger ses marques de commerce*, Cowansville, Éditions Yvon Blais, 2010; Lisa VEASMAN, « 'Piggy Backing' on the Web 2.0 Internet Copyright Liability and Web 2.0 Mashups », [2008] 30 *COMM/ENT* 311-337.

producteur et consommateur, ce qui dramatise la question des statuts et responsabilités respectives des uns et des autres[12].

2. Les risques de configuration

Les environnements du Web 2.0 comportent certains risques qui ne découlent pas exclusivement de la volonté ou du comportement du maître de site ou de l'usager. La façon dont sont configurés les environnements peut faciliter l'accomplissement de gestes qui peuvent se révéler illicites. Par exemple, la facilité technique avec laquelle il est possible d'introduire un contenu sur un blogue ou sur un site de partage de documents audio ou vidéo est, en elle-même, génératrice de risques. Cette normativité par défaut facilite des gestes qui peuvent aisément contrevenir à d'autres règles, telles que celles relatives à la propriété intellectuelle.

Par exemple, on a fréquemment signalé l'importance des effets d'agrégation et des capacités des moteurs de recherche[13]. L'information – même de caractère public – peut plus facilement être trouvée puis agglomérée de manière à déduire des informations qui relèvent de la vie privée. De ce fait, les risques pour la vie privée changent d'échelle sur Internet.

La configuration même d'Internet, qui ignore les frontières territoriales, engendre des risques. Par exemple, plusieurs fonctions du Web 2.0 permettent l'utilisation hors contexte de l'information. La conception des sites de réseautage personnel provient d'une reconnaissance qu'il y a, pour chaque personne, des lieux différenciés au sein desquels le statut des informations ne sera pas forcément le même. Par exemple, il pourra être fautif de reprendre un commentaire formulé dans l'intimité et de le diffuser à un cercle plus vaste.

Internet n'est pas un environnement univoque : on y trouve des lieux de toutes sortes. Certains comportent plus de risques pour la vie privée de personnes qui les fréquentent. Par exemple, les sites de réseautage social sont configurés de manière à favoriser la rencontre et la mise en relation de personnes via leurs réseaux sociaux.

On peut enfin signaler la volatilité des contenus circulant dans plusieurs environnements du Web 2.0. Les contenus peuvent être modifiés par un usager et recombinés à l'infini. Les usagers ont la possibilité d'intervenir sur les contenus et d'y apporter des modifications. Le contenu ne peut pas être tenu pour définitif au sens où l'on avait l'habitude de le postuler pour les publications éditées. Le processus d'édition se présente désormais en un mouvement continu dans lequel une pluralité d'intervenants de statuts différents peuvent intervenir.

---

12 Pierre-Yves GAUTIER, « Le contenu généré par l'utilisateur », *LÉGICOM*, no. 41, 2008/1, p. 1-7.

13 Daniel J. SOLOVE, « Access and Aggregation: Public Records, Privacy and the Constitution, » [2002] 86 *Minn. L. Rev.,* 1137-1218.

3. Les risques et enjeux de régulation

La régulation elle-même – qu'elle résulte des configurations techniques, de l'activité des acteurs eux-mêmes ou des règles mises en place par les autorités étatiques - est génératrice de risques. Les règles ont évidemment pour objectif d'être observées. Mais en pratique, les acteurs ne se conformeront pas à des règles qui vont à l'encontre de leurs intérêts s'ils perçoivent que le risque de devoir subir des conséquences adverses pour leur non-conformité est faible.

La superposition des rôles et des catégories tels que définis dans la réglementation applicable dans les différents territoires accroît le risque. Jan Trzaskowski observe que « *In the absence of globally accepted standards for geographical delimitation of content on the Internet, the infringement of foreign law is a risk which businesses inevitably will run when carrying out electronic commerce*. »[14] Dans les environnements Web 2.0, les différents acteurs occupent des positions et tiennent des rôles qui changent. Cette volatilité des rôles tenus par les acteurs peut rendre problématique la détermination des responsabilités. Il en découle une difficulté à identifier qui « répond » des contenus et activités. Ce relatif déficit d'« imputabilité » tend à accroître la relative incertitude quant à l'identité de ceux qui auront à répondre d'un fait dommageable ou illicite.

Les usages et les pratiques en réseau engendrent également des régulations qui peuvent être génératrices de risques pour certains usagers. Mettre en ligne un site dans lequel il est loisible à n'importe quel usager d'introduire des propos ou images portant sur une autre personne constitue assurément une régulation par défaut qui engendre des risques pour les tiers éventuellement concernés par les documents mis en ligne.

Les usagers agissent en réseau. Ils interagissent et, du coup, développent des solutions aux problèmes rencontrés. Ils développent des façons de faire afin de minimiser leurs risques. Dans plusieurs situations, ils vont mettre en place un ensemble de règles qui encadrent le déroulement des activités. En somme, les normes elles-mêmes sont en partie produites dans le cadre des interactions en réseau[15] mais, une fois établies, ces normes engendrent forcément des risques pour les autres acteurs.

---

[14] Jan TRZASKOWSKI, « Legal Risk Management in a Global Electronic Marketplace », [2006] 49 *Scandinavian Studies in Law,* 319-337, p. 320.

[15] David D. JOHNSON, Susan P. CRAWFORD & John G. PALFREY jr, « The Accountable Internet: Peer Production of Internet Governance », [2004] 9 *Virginia Journal of Law & Technology*, 1-32.

II- Les responsabilités découlant des activités se déroulant sur le Web 2.0

Lorsqu'on s'interroge sur les responsabilités, on se demande qui est tenu de répondre des situations problématiques qui se manifestent. On veut savoir qui est responsable…, qui doit répondre de ce qui ne s'est pas adéquatement déroulé.

Dans ce chapitre, on explique comment sont définies et réparties les responsabilités de ceux qui prennent part à des activités se déroulant sur Internet.

La responsabilité à l'égard des environnements d'Internet se décline à plusieurs niveaux. Il y a tout d'abord la responsabilité de décider de mettre en place des environnements de diffusion ou d'interaction. Dans le secteur public, certaines décisions peuvent être prises au niveau de l'organisme. Dans le secteur privé, les instances dirigeantes ont à évaluer les enjeux et risques et à décider en conséquence.

Cependant, l'Internet du Web 2.0 habilite tout usager à diffuser ou à interagir. Il pourra fréquemment arriver qu'à même les environnements génériques disponibles ou en-dehors de ceux-ci, des employés prennent l'initiative de la mise en place d'outils et d'environnements d'interaction.

Chacune des personnes susceptibles d'interagir en ligne doit être au fait des enjeux et risques associés aux activités se déroulant dans le cyberespace. La grande liberté dont jouissent les individus sur Internet implique pour eux l'obligation de prendre les précautions nécessaires afin de se prémunir contre les risques inhérents à la communication en ligne.

L'usage d'Internet met en jeu différents types de responsabilités. Dans les environnements du Web 2.0, tous ont une importante capacité de mettre en ligne des informations de toute nature. À ce pouvoir considérable correspondent nécessairement des responsabilités. Les entreprises et les organismes publics, de même que leurs préposés, assument des responsabilités à différents titres.

La question de la responsabilité prend toute son importance dans des situations où un dommage a été causé. Évidemment, on parle ici de situations exceptionnelles. Dans la plupart des cas, il n'y a pas d'incident et les activités n'engendrent aucune conséquence dommageable. C'est pour le nombre restreint de situations où des torts ont été causés que l'on s'enquiert des responsabilités qui incombent aux différents acteurs et que l'on se donne des consignes afin d'éviter les incidents dans toute la mesure du possible.

La responsabilité des acteurs du Web 2.0 se décline en plusieurs catégories. On peut être responsable d'avoir transgressé ou ignoré les valeurs de l'entreprise ou les engagements moraux pris par une personne ou une organisation, mais la responsabilité peut également découler de la transgression d'une loi ou d'une autre règle qui s'impose de façon obligatoire.

La **responsabilité politique** peut être en cause dès lors que survient un événement déplorable, fut-il un incident isolé. On pourra montrer du doigt ceux ou celles qui « auraient dû » ou qui « n'auraient pas dû »! On est alors dans le domaine de la responsabilité politique. Les perceptions de l'opinion publique sont ici cruciales. Le fait de pouvoir prétendre que l'on n'a pas enfreint d'exigence d'une loi est de peu de secours.

Il suffit qu'un incident particulièrement médiatique se produise pour que les médias d'information s'interrogent sur les politiques, ou l'absence de politiques d'une entreprise ou d'un organisme à l'égard des usages qui peuvent être faits d'Internet. Dans ce genre de circonstances, toutes les organisations doivent être en mesure d'exposer quelles lignes de conduite elles demandent de suivre, quelles précautions sont prises, quelles approches sont privilégiées et quels sont les moyens d'éviter que des incidents se reproduisent.

Un deuxième chef de responsabilité est celui de la **responsabilité légale**. En cas d'incident, il faut déterminer qui répond des fautes et des dommages, qui est responsable de la violation de la loi. Dans l'environnement Internet relevant d'une entreprise ou d'un organisme, ou encore lorsque des activités se déroulent sur Internet, se pose nécessairement la question de savoir qui répond de ce qui s'y passe, des faits et gestes qui y surviennent. Dans ce schéma, l'entreprise a une responsabilité pour ce qu'elle décide de communiquer.

L'entreprise ou l'organisme public peut aussi avoir à répondre de ce qui se déroule dans les environnements du Web 2.0 à titre d'employeur. Étant donné que les personnes oeuvrant au sein d'une organisation ont désormais accès à la plupart des espaces de communication en réseau, certains de leurs faits et gestes peuvent engendrer des conséquences pour l'organisation.

L'entreprise peut aussi devenir responsable en tant qu'intermédiaire dans un processus de communication sur Internet. À l'égard des employés ou des clients, plusieurs organisations agissent uniquement comme intermédiaires. Ce sont les employés ou les clients qui assument la maîtrise des communications dans les environnements d'Internet et l'entreprise ou l'organisme public n'agit qu'à titre d'hébergeur ou encore se limite à procurer la connectivité ou des facilités de transmission. Dans de telles situations, la responsabilité de l'organisation sera moindre.

A. La responsabilité des individus

Dans la plupart des environnements du Web 2.0, ce sont les individus qui ont la maîtrise de ce qu'ils mettent en ligne. Dans plusieurs des situations, le participant agit seul sur Internet. Il peut transmettre des informations, accéder à des forums, révéler des informations sur lui-même ou sur d'autres dans des sites de réseaux sociaux, naviguer de manière à accéder à des informations de toute nature. Les environnements du

Web 2.0 laissent une grande marge d'autonomie aux individus. Ceux-ci sont à même de poser des gestes pouvant avoir des conséquences importantes. L'une des premières habiletés qu'il faut posséder est de connaître les responsabilités incombant à une personne qui transmet ou reçoit des informations sur Internet. Par exemple, révéler à la grandeur d'Internet une information sur soi-même, sur une autre personne ou sur son employeur peut entrainer de graves répercussions.

Ainsi, la personne ayant personnellement posé le geste fautif est généralement la première à en assumer la responsabilité. Lorsqu'elle est douée de raison, la personne qui choisit de mettre en ligne une information ou se comporte de manière à exercer un contrôle sur la diffusion de celle-ci assume la responsabilité découlant de son caractère illicite.

C'est pourquoi l'on attache tant d'importance à l'information des participants. Ceux-ci se trouvent dotés de facultés considérables de produire, de diffuser et de partager de l'information. Ils doivent impérativement être au fait des enjeux et risques associés à leurs activités en ligne.

> ***Les Informations à communiquer pour aider les participants à une activité sur Internet à prendre conscience de leurs responsabilités***
>
> - *Une description de l'activité, ses objectifs, les modalités de son déroulement.*
> - *Une description des risques spécifiques qui y sont associés.*
> - *Une liste de précautions à prendre afin de minimiser les risques.*
> - *Des consignes sur ce qu'il convient de faire en cas de situation problématique.*
> - *Un ensemble de recommandations afin de minimiser les risques lors de l'utilisation d'Internet à partir de lieux situés en dehors de ceux de l'entreprise ou de l'organisme.*

B. L'entreprise ou l'organisme public comme employeur

Plusieurs enjeux découlent du statut d'employeur[16]. Les organisations comptent sur la loyauté de leurs employés. Ces derniers peuvent poser des gestes qui engagent la responsabilité de leur employeur. Plusieurs applications associées au Web 2.0 confèrent aux personnes oeuvrant au sein des organisations des capacités sans précédent de traiter des informations. Il est plus difficile de prendre pour acquis que les organisations peuvent exercer un contrôle étendu à l'égard de tous et chacun des éléments d'information qui circulent dans l'entreprise ou à l'extérieur en provenance de celle-ci.

---

[16] Sylvain LEFEBVRE « Naviguer sur Internet au travail : et si on nageait en eaux troubles ? », *Développements récents en droit du travail,* 2008, EYB2008DEV1485; Carolyn ELEFANT, "The 'Power' of Social Media:Legal Issues & Best Practices for Utilities Engaging Social Media", (2011) 32 *Energy Law Journal,* 1, p.11 et ss.

1. Le recours aux sites Web 2.0 dans les pratiques d'embauche

Lors des embauches, le recours aux informations disponibles en ligne à l'égard des personnes qui proposent leur candidature est devenu pratique courante[17]. Une étude commandée par Microsoft et réalisée par Cross-Tab en décembre 2009, démontre que 79 % des recruteurs américains consultent Internet pour évaluer la réputation des candidats. En effet, 70 % des recruteurs interrogés ont affirmé avoir rejeté des candidats sur la base de l'information trouvée en ligne. L'étude indique toutefois que seulement 7 % des Américains pensent que l'information disponible sur le Web peut influencer leurs démarches d'emploi. D'autre part, 85 % des recruteurs ont affirmé qu'une réputation positive sur Internet influençait leur décision quant à l'embauche de candidats[18].

Les sites de réseautage social peuvent avoir un impact sur l'obtention d'un emploi. En effet, selon une étude menée en 2009, 28 % des employeurs canadiens consultent les sites de réseautage social pour en savoir plus sur les candidats qui postulent pour un emploi au sein de leur entreprise. Ainsi, 14 % des employeurs « branchés » affirment avoir trouvé du contenu sur les sites de réseautage social qui a favorisé la candidature d'un individu. Toutefois, 26 % ont plutôt découvert du matériel qui a entraîné l'élimination d'un candidat (photos compromettantes, révélations concernant l'usage d'alcool ou de drogues, renseignements ou commentaires inappropriés concernant un ancien employeur). Les sites de réseautage social semblent donc de plus en plus constituer un outil à double tranchant[19].

Or, des risques sont associés à ces utilisations des informations relatives à des candidatures.

a) La discrimination dans les offres d'emploi

Plusieurs législations interdisent les offres d'emploi manifestant une préférence fondée sur le sexe, la race, l'origine nationale, la religion, l'âge, l'orientation sexuelle ou d'autres motifs prohibés de discrimination. Ces dispositions interdisent évidemment des mentions explicites révélant des préférences discriminatoires. Mais le recours à certains environnements de diffusion pour faire connaître des offres d'emploi peut être indicateur d'une intention de discriminer. Par exemple, aux États-Unis, les autorités ont mis en garde contre le recours à des publications ciblant principalement les hommes ou

---

[17] INITIATIVE CANADIENNE DES CONSOMMATEURS, *Comprendre la gestion et la restauration de la réputation sur internet*. Ottawa, Novembre 2011, <www.cci-icc.ca/CCI-pdf/CCI-fr-reputation-sur-internet.pdf >.

[18] « Research shows online reputations matter », *Microsoft Data Privacy Day*, http://www.microsoft.com/privacy/dpd/default.aspx

[19] Gilbert LEDUC, « Gare aux confidences sur Internet », *Le Soleil*, 28 août 2009, en ligne : http://technaute.cyberpresse.ca/nouvelles/internet/200908/27/01-896475-gare-aux-confidences-sur-internet.php .

d'autres catégories ciblées de personnes pour publier des offres d'emploi. Certains ont avancé que le recours à des réseaux sociaux fréquentés par des catégories d'usagers spécifiques pourrait être contesté comme indiquant une intention de discriminer à l'embauche[20].

b) L'utilisation des informations glanées sur le profil d'un candidat potentiel pour éclairer une décision d'embauche

Les informations personnelles dévoilées sur un site de réseautage social peuvent être utilisées de plusieurs façons. Ainsi, il a été fait état des risques pouvant découler de la consultation décontextualisée, notamment par des employeurs, d'informations ou d'images consignées dans les sites de réseaux sociaux[21]. Par exemple, des entreprises peuvent surfer sur les espaces personnels pour en apprendre plus sur des candidats avant de les embaucher[22].

L'accès par une entreprise à des informations relevant de l'intimité des personnes ayant proposé leur candidature à un emploi peut poser des enjeux de protection de la vie privée. Si l'on ne demande pas l'autorisation à un candidat pour rechercher des informations sur son compte, il y a risque de se placer dans une position d'intrusion injustifiée dans la vie privée. Au minimum, une organisation doit informer les personnes concernées de ses pratiques en matière de recherche d'information et, en tout état de cause, être en mesure de démontrer le caractère légitime des recherches d'information qu'elle mène à l'égard d'individus. De façon générale, il est licite de rechercher des informations reflétant le jugement d'un candidat ou sa capacité à faire le travail. Mais il doit exister un lien de connexité avec l'emploi.

L'un des principaux risques à évaluer dans des situations où une organisation recherche et utilise des informations obtenues dans des environnements en ligne, comme des sites de réseaux sociaux, est la fiabilité des informations obtenues. Plusieurs éléments d'information qui peuvent se trouver en ligne à l'égard d'un individu n'ont pas nécessairement été validés. De plus, des informations peuvent avoir une signification dans un contexte déterminé et se révéler ambigües dans un autre contexte. Par exemple, une photo d'un groupe de personne en train de célébrer au cours de ce qui a l'apparence d'une fête bien arrosée peut être perçue comme un indice de la sociabilité des individus impliqués ou un indice de leur propension à fêter…

---

20 TALEO.COM, *Guide du recrutement sur les réseaux sociaux*, http://www.fichier-pdf.fr/2011/11/09/guide-du-recruteur-sur-les-reseaux-sociaux/guide-du-recruteur-sur-les-reseaux-sociaux.pdf.

21 Darryn Cathryn BECKSTROM, « Who's Looking at your Facebook Profile ? The Use of Student Conduct Codes to Censor College Students' Online Speech », [2008] 45 *Willamette L.Rev.*, 261-312.

22 Samantha L. MILLIER, « The Facebook Frontier : Responding to the Changing Face of Privacy on the Internet », [2008-2009] 97 *Kentucky L. J.*, 541-564,544.

2. Les limites au contrôle de l'employeur sur l'usage du Web 2.0 par les employés

Tout employeur est tenu à des obligations qui peuvent impliquer une supervision ou une sensibilisation des employés.

La mission ou le mandat de l'entreprise ou de l'organisme peut impliquer certains enjeux et risques. Ainsi, une entreprise tenue de garantir la confidentialité des informations relatives à ses clients doit prendre des mesures afin de s'assurer que ce devoir de confidentialité est respecté par tous. À défaut de prendre des précautions proportionnées aux obligations auxquelles elle est tenue, une organisation aura à répondre des bris de confidentialité.

Tous les employés ont droit, en vertu des législations sur le travail, à un environnement de travail exempt de harcèlement. Tout employeur a donc le devoir de s'assurer que les actions de harcèlement émanant de l'environnement de travail soient rapidement détectées et éradiquées. L'entreprise doit faire en sorte que le harcèlement cesse dès qu'elle en a connaissance.

a) La surveillance des activités des employés

Il est bien établi qu'un employé a droit à la vie privée, et ce, même sur son lieu de travail[23]. Mais il y a des circonstances où il est légitime pour un employeur de surveiller les gestes de ses employés. La surveillance doit être fondée sur des motifs raisonnables. Pour déterminer si les motifs sont raisonnables, on s'enquiert du lien rationnel entre les périls contre lesquels on cherche à se protéger et l'on s'assure que les mesures sont proportionnées aux enjeux[24].

L'entreprise doit avoir des motifs raisonnables pour recueillir les informations sur l'ordinateur de l'employé[25]. Par exemple, une diminution significative de la production d'un employé pourrait justifier la surveillance de son poste de travail[26]. En l'absence de tout soupçon, la recherche par un employeur d'indices d'une mauvaise utilisation d'Internet sur un ordinateur d'un employé en espérant y trouver quelque chose pour ensuite se servir des éléments trouvés pour justifier son intrusion a posteriori est une pratique contestable.

---

23 *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, [1999] R.J.Q. 2229 (C.A.)

24 Diane VEILLEUX, « Le droit à la vie privée – sa portée face à la surveillance de l'employeur », (2000) 60 *R. du B.* 3, 36-45

25 Yves SAINT-ANDRÉ, « Le respect du droit à la vie privée au travail : mythe ou réalité? », (2004) EYB2004DEV408

26 *Syndicat des fonctionnaires municipaux de Montréal (S.C.F.P.)* c. *Ville de Montréal*, D.T.E. 99T-478 (T.A.)

L'exigence de proportionnalité commande que les méthodes utilisées pour surveiller l'employé constituent une atteinte minimale au droit à la vie privée de l'employé[27]. Un employeur ne pourrait donc surveiller continuellement tous les faits et gestes de ses employés sur Internet. C'est seulement lorsque ces conditions sont réunies que l'employeur est en droit de surveiller les activités d'un employé sur Internet. Autrement, il risque de contrevenir à l'article 46 de la *Charte des droits et libertés de la personne*[28] qui prévoit que tout employé a le droit à des conditions de travail justes et raisonnables.

Un employé qui utilise les ressources de son employeur à des fins personnelles, comme les ordinateurs ou l'accès à Internet, peut s'exposer à des sanctions. L'usage d'Internet pour aller visiter des sites Web 2.0 ou encore pour y contribuer, lorsque ce n'est pas dans le cadre du travail, peut donc être sanctionné par l'employeur au même titre que toute autre utilisation inappropriée du réseau.

Alors que certaines entreprises tolèrent les utilisations privées d'Internet, d'autres établiront plutôt une politique d'utilisation d'Internet limitant la faculté des employés d'utiliser le réseau. Quelle que soit la forme que prend l'avertissement, un employeur qui ne veut pas que ses installations soient utilisées à des fins privées doit habituellement en avertir ses employés avant d'appliquer des sanctions[29].

Une entreprise ou un organisme public peut indiquer à ses employés qu'il est inapproprié de naviguer sur des sites comme YouTube[30], MySpace[31] ou encore Facebook[32] sur son lieu de travail. L'employé doit savoir que cette pratique est interdite, d'où la nécessité d'un avertissement de la part de l'employeur.

Plusieurs situations d'investigations ou d'utilisation contestable des données personnelles circulant dans les sites de réseaux sociaux ont été recensées et dénoncées. Par exemple, il a été fait état de la consultation décontextualisée, notamment par des employeurs, d'informations ou d'images consignées dans les sites de réseaux sociaux[33]. Par exemple, une adolescente britannique a été congédiée pour avoir exprimé sur Facebook qu'elle trouvait son emploi ennuyant. Alors que l'employeur le perçoit comme

---

27 Yves SAINT-ANDRÉ, « Le respect du droit à la vie privée au travail : mythe ou réalité ? », (2004) EYB2004DEV408

28 L.R.Q., c. C-12

29 *Fiset* c. *Service d'administration P.C.R. Ltée*, [2003] R.J.D.T. 361 (C.R.T.)

30 http://www.youtube.com/

31 http://www.myspace.com/

32 http://www.facebook.com/

33 Darryn Cathryn BECKSTROM, « Who's Looking at your Facebook Profile ? The Use of Student Conduct Codes to Censor College Students' Online Speech », [2008] 45 *Willamette L.Rev.*, 261-312.

une rupture du lien de confiance, la jeune femme affirme qu'elle n'était pas malheureuse au travail et soutient qu'elle n'avait pas nommé l'employeur[34].

Dans *West Coast Mazda v. United Food and Commercial Workers International Union, Local 1518*[35], la Commission des relations de travail de Colombie-Britannique a estimé qu'un employé n'avait pas beaucoup d'expectative de vie privée lorsqu'il diffuse des commentaires sur sa page Facebook. Cette décision est l'une des premières à confirmer la validité d'un congédiement consécutivement à un propos affiché sur un site de réseau social[36]. La Commission a conclu que l'employeur était justifié de mettre fin à l'emploi d'un salarié ayant affiché des commentaires très critiques au sujet de l'entreprise de l'employeur. Ces propos avaient été rendus disponibles à un groupe d'environ 377 personnes incluant d'autres employés de l'entreprise. Ainsi diffusés, ces commentaires ne pouvaient être considérés comme analogues aux propos tenus entre collègues de travail dans le cadre de discussions sur les lieux de travail.

Si elle entend s'inscrire dans une logique ouverte caractéristique du Web 2.0, l'entreprise ou l'organisme public visera à promouvoir une utilisation responsable des environnements du Web 2.0 par ses employés. Le défi est alors de s'assurer que les employés sont bien au fait des enjeux et risques associés aux différentes activités qu'ils sont susceptibles de mener sur Internet. En somme, plus les individus détiennent des pouvoirs importants pour diffuser des informations, plus ils doivent être familiarisés avec les enjeux et risques pouvant découler de leur activité.

b) Les activités de l'employé en-dehors du travail

Il est possible d'utiliser les environnements du Web 2.0 en tout temps. Le Web 2.0 modifie radicalement les références spatiales et temporelles. Avec l'apparition d'Internet puis du Web 2.0, l'espace des organisations s'est élargi en une communauté de pratique de dimension planétaire qui a fait éclater les murs physiques et les cadres traditionnels dans lesquels se déroulent les activités de l'entreprise ou de l'organisme public. Il est donc pratiquement hors de question pour une organisation d'interdire à ses employés toute utilisation des environnements d'Internet comme les réseaux sociaux. Mais étant donné l'ubiquité qui caractérise les environnements du Web 2.0, il faut envisager les enjeux et risques de façon globale, et non plus uniquement au regard de l'espace physique des lieux de travail.

---

34 « Sacked For Calling Job Boring On Facebook », *Sky News*, 27 février 2009, http://news.sky.com/skynews/Home/UK-News/Facebook-Sacking-Kimberley-Swann-From-Clacton-Essex-Sacked-For-Calling-Job-Boring/Article/200902415230508

35 2010 CanLII 62482 (BC L.R.B).

36 Gary CLARKE, « Employees Terminated for Cause for Facebook Postings », Stikeman Elliot, *Canadian Employment & Pension Law*, November 12, 2010, http://www.canadianemployment pensionlaw.com/ termination/a-recent-decision-of-the/ .

Si, *a priori*, la responsabilité de l'entreprise s'applique sur les lieux physiques de l'établissement, force est de constater que la généralisation des outils du Web 2.0 et la disponibilité accrue d'outils dotés d'importantes capacités de diffusion posent la question de savoir où commencent et où s'arrêtent le droit et la responsabilité de l'entreprise.

La délocalisation accompagnée de la détemporalisation de l'espace associé à l'entreprise requièrent de s'interroger sur les responsabilités des employés et des dirigeants pour les gestes fautifs commis en dehors de l'espace physique de l'entreprise.

Or, pour que la responsabilité de l'employeur soit engagée, il faut qu'un événement ayant causé préjudice soit survenu sur les lieux du travail et à l'occasion du travail[37].

S'agissant des entités oeuvrant dans le monde de l'éducation, tant aux États-Unis qu'au Canada, les tribunaux ont reconnu que les autorités scolaires peuvent appliquer des sanctions aux enseignants ou aux élèves pour des activités fautives s'étant déroulées sur Internet et ce, même si les gestes ont été posés entièrement en dehors des espaces relevant de l'école[38]. En fin de compte, la délocalisation et la détemporalisation de l'espace tendent à s'accompagner d'un ajustement conséquent des pouvoirs reconnus aux employeurs de prendre les mesures raisonnablement nécessaires afin de faire cesser des comportements en ligne qui sont de nature à engendrer un effet délétère sur le milieu de travail.

3. La responsabilité de l'entreprise ou de l'organisme public pour la conduite de l'employé

Les entreprises et organismes ont une responsabilité pour les gestes et les omissions des personnes à leur service. En tant qu'employeur, une entreprise ou un organisme public assume une responsabilité pour les gestes posés par ses employés dans l'exercice de leurs fonctions.

Devant cette situation, plusieurs organisations ont pris la décision d'interdire tout simplement l'usage d'Internet ou de certains environnements en ligne. Mais, une telle approche tend de plus en plus à se révéler inefficace. Avec la popularité croissante des outils portables comme les téléphones dits « intelligents », les individus peuvent se trouver en mesure de communiquer, même en dehors des environnements sous le contrôle des organisations.

Il paraît plus efficace de promouvoir une utilisation responsable des environnements du Web 2.0. La nature même du Web 2.0 habilite les individus à accéder et à maîtriser de

---

37 *G.M. et Compagnie A*, 2010 QCCLP 8780 (CanLII), 2 décembre 2010, http://www.canlii.org/fr/qc/qcclp/doc/2010/2010qcclp8780/2010qcclp8780.html

38 *Ross c. Conseil scolaire du district n° 15 du Nouveau*□*Brunswick* [1996] 1 R.C.S. 825

plus en plus d'informations. Dans une telle perspective, promouvoir une approche par laquelle l'ensemble des individus sont responsabilisés semble plus à même de protéger l'entreprise ou l'organisme public contre les comportements préjudiciables.

C. Les employés comme utilisateurs du Web 2.0

En tant qu'utilisateurs des environnements du Web 2.0, les employés ont, à l'égard de leur employeur une obligation de loyauté : ils doivent s'abstenir de poser des gestes qui minent la confiance qui doit exister entre un employeur et un employé. Une telle obligation connaît des intensités variables selon le type d'emploi et l'intensité du lien de subordination qui est inhérente aux différents types d'emploi. Un emploi d'exécution de tâches définies implique une marge d'appréciation moins étendue qu'un emploi de création impliquant une large liberté d'action.

1. Les obligations des employés

Les employés ont l'obligation de protéger l'information confidentielle, de préserver les secrets de commerce ou autres secrets inhérents à la conduite des activités de l'employeur.

Les lois obligent aussi les employés à se garder de toute activité de harcèlement à l'endroit de collègues de travail. Les employés ne peuvent intimider, diffamer ou porter atteinte à la vie privée et aux autres droits des autres employés.

L'intensité de ces obligations et la rigueur de la surveillance et des sanctions connaissent des variations, selon la place occupée par les employés au sein de l'organisation.

Dubois, Pelletier et Poirier distinguent les employés mandatés et les employés non mandatés. Les employés mandatés sont ceux qui « sont officiellement mandatés par l'organisation pour la représenter sur les médias sociaux »[39]. Dans cette catégorie d'intervenants nécessairement plus familiers avec les enjeux et risques associés aux activités prenant place dans les environnements du Web 2.0, les auteurs Dubois, Pelletier et Poirier distinguent les représentants officiels, les gestionnaires de communautés et les ambassadeurs.

Les représentants officiels « sont les employés dont la présence sur les médias sociaux est justifiée par le mandat très clair de représentation de leur organisation dans leur domaine d'expertise ». Leur importante présence dans les médias sociaux à titre de

---

[39] Didier DUBOIS, Emilie PELLETIER et Katherine POIRIER, *Comment bâtir votre politique d'utilisation des médias sociaux*, Cowanville, Éditions Yvon Blais, 2011, p. 60.

représentants officiels « *lie de manière étroite leurs activités numériques et l'image de leur employeur* »[40].

Pareillement, le gestionnaire de communauté agit comme ressource centrale de l'organisation dans la communication dans les environnements d'interaction dans lesquels elle est présente. Il est donc forcément en position de porte-parole de l'organisation. Les employés à qui l'organisation « a donné mandat de partager leur expertise en tant que représentants officiels de l'entreprise » sont désignés par le vocable d'« ambassadeurs » par Dubois, Pelletier et Poirier[41]. Ils se trouvent à la fois en position de représentant de l'organisation, mais en même temps « agissent comme des agents libres qui gèrent leur propre groupe, indépendamment des objectifs de l'entreprise »[42]. L'organisation doit s'assurer que leurs faits et gestes demeurent en cohérence avec ses orientations.

Les employés peuvent intervenir sur des questions qui concernent l'organisation sans être mandatés pour ce faire. Dubois, Pelletier et Poirier identifient trois types d'employés : les enthousiastes agissant habituellement par fierté d'appartenir à l'organisation, les inconscients qui « n'hésitent pas à promouvoir des comportements marginaux sur les médias sociaux tout en mentionnant le nom de l'organisation pour laquelle ils travaillent » et les frustrés, ceux qui décident de s'en prendre à l'employeur en utilisant les plateformes du Web 2.0[43]. Les employés doivent être sensibilisés aux risques de formuler des commentaires, même de bonne foi, concernant leur environnement de travail.

2. Les responsabilités des employés découlant d'agissements sur un site Web 2.0

Il n'y a pas seulement l'utilisation d'Internet à des fins privées qui peut présenter des risques au niveau du travail. En effet, il peut également être risqué de parler de son travail, de ses collègues ou encore des clients de son employeur sur un site Web 2.0, en particulier sur un blogue. Les cas de congédiement, suite à des propos tenus sur un blogue, démontrent le type de risques de ces environnements.

---

40 Didier DUBOIS, Emilie PELLETIER et Katherine POIRIER, *Comment bâtir votre politique d'utilisation des médias sociaux*, Cowanville, Éditions Yvon Blais, 2011, p. 60.

41 Didier DUBOIS, Emilie PELLETIER et Katherine POIRIER, *Comment bâtir votre politique d'utilisation des médias sociaux*, Cowanville, Éditions Yvon Blais, 2011, p. 61.

42 Didier DUBOIS, Emilie PELLETIER et Katherine POIRIER, *Comment bâtir votre politique d'utilisation des médias sociaux*, Cowanville, Éditions Yvon Blais, 2011, p. 61.

43 Didier DUBOIS, Emilie PELLETIER et Katherine POIRIER, *Comment bâtir votre politique d'utilisation des médias sociaux*, Cowanville, Éditions Yvon Blais, 2011, p. 61.

On signale des situations dans lesquelles des personnes ont été congédiées suite à des propos tenus dans un blogue[44]. Par exemple, en Ontario une préposée aux bénéficiaires avait publié sur son blogue des renseignements sur des patients de même que des propos injurieux sur l'administration ainsi que sur certains employés de l'établissement qui l'employait[45]. Elle a été congédiée pour rupture de la politique de confidentialité de l'établissement et pour insubordination[46].

La politique de confidentialité est un véhicule important afin de communiquer aux employés les balises quant à ce qui peut être révélé. En cas de transgression à cette politique, l'employeur peut alors imposer une sanction, qui peut aller d'un simple avertissement jusqu'au congédiement. Dans les cas graves, même en l'absence de politique de confidentialité, le dévoilement de certains renseignements obtenus dans le cadre du travail peut être sanctionné, par exemple si un avocat brise le secret professionnel pour dévoiler sur son blogue des confidences reçus dans le cadre d'une consultation[47].

L'un des risques importants à parler de son travail sur Internet est d'être accusé d'insubordination. L'insubordination peut se définir comme étant un refus de se conformer à la discipline générale de l'entreprise, d'effectuer un travail ou d'exécuter un ordre légitime de l'employeur dans l'intention de résister à l'autorité ou de la défier[48]. Des commentaires désobligeants sur un blogue concernant les décisions d'un employeur ou encore des insultes à l'endroit d'un supérieur hiérarchique peuvent être considérés comme constituant de l'insubordination[49]. Dans de pareilles situations, l'employeur peut avoir un motif suffisant pour congédier l'employé fautif.

Un autre risque inhérent aux environnements du Web 2.0 est celui de porter atteinte à la vie privée de personnes de l'entourage. En effet, en dévoilant des informations sur un

---

44 Voir, par exemple, pour les États-Unis, les sites http://www.michaelhanscom.com/ et http://queenofsky.journalspace.com/, qui sont des blogues tenus par des employés qui se sont fait congédier (sites visités le 19 décembre 2011). Pour la France, voir le cas de Catherine Sanderson (Bruno GUGLIELMINETTI. « Technologie – Bloguer à ses risques et périls », In *LeDevoir.com*, [En ligne]. http://www.ledevoir.com/2007/04/02/137888.html, (Page consultée le 19 décembre 2011))

45 *Chatham-Kent (Municipality)* c. *National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127 (Clarke Grievance)*, [2007] O.L.A.A. (Quicklaw) n° 135

46 *Chatham-Kent (Municipality)* c. *National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127 (Clarke Grievance)*, [2007] O.L.A.A. (Quicklaw) n° 135

47 *Loi sur le Barreau*, L.R.Q., c. B-1, art. 131

48 « Insubordination » Office québécois de la langue française, In *Le grand dictionnaire terminologique*, [En ligne]. http://www.granddictionnaire.com, (Page consultée le 19 décembre 2011)

49 *Chatham-Kent (Municipality)* c. *National Automobile, Aerospace, Transportation and General Workers Union of Canada (CAW-Canada), Local 127 (Clarke Grievance)*, [2007] O.L.A.A. (Quicklaw) n° 135

collègue ou sur un client, il y a risque de porter atteinte à sa vie privée. Il est possible également de violer le droit à l'image d'une personne en publiant sa photo sans son consentement.

D. La responsabilité découlant de l'activité des tiers - clients, bénévoles, fans de produits de l'entreprise, partenaires d'affaires

Internet facilite la contribution de tiers aux contenus proposés en ligne. Les principaux contextes de diffusion sur Internet possèdent des caractéristiques variables. De ces différentes caractéristiques peuvent résulter des différences significatives dans l'intensité de la responsabilité incombant aux entités qui exploitent des sites.

Dans le « Web 2.0 », il existe des situations où le contenu est entièrement validé par l'entreprise ou l'organisme qui a la maîtrise du site. Mais il existe aussi des environnements ou des sites dans lesquels le contenu est en totalité ou en partie généré par des tiers. Plusieurs environnements du Web 2.0 permettent aux membres du public d'interagir avec l'entreprise ou l'organisme public ou encore de faire circuler des informations ou partager des avis et impressions au sujet d'une entreprise ou organisme public ou encore les produits et services qu'ils proposent au public.

Ces tiers, utilisateurs, internautes « amateurs » ou « professionnels » introduisent des documents sur un site. Il peut s'agir de clients de l'entreprise ou de personnes qui ont un intérêt pour ses activités. Enfin, l'entreprise ou l'organisme peut avoir des sites qui ne font qu'héberger des contenus qui sont sous la seule maîtrise des usagers.

Au plan de la responsabilité, la diffusion sur Internet sur un site s'analyse comme toute autre diffusion au public. Lorsqu'un site est « édité », la personne qui exerce l'autorité éditoriale – l'éditeur – répond de tous et chacun des éléments qui constituent la publication. Mais plusieurs sites associés à l'univers du « Web 2.0 » proposent différents contenus émanant de tiers.

Or, il existe une importante différence, au regard de la responsabilité, entre les contenus émanant de l'entité qui exerce le contrôle éditorial d'un site et les contenus émanant de tiers. Ainsi, lorsqu'une entreprise ou un organisme diffuse des contenus émanant de tiers, qu'il s'agisse de clients, ou de « fans » de l'entreprise, il importe de déterminer le rôle que tient l'entreprise ou l'organisme au regard de ces contenus mis en ligne par des tiers.

La responsabilité de l'entreprise ou de l'organisme ne sera pas la même, selon qu'il s'agit d'informations mises en ligne suite à sa décision, ou encore d'informations mises en ligne par décision d'une personne qui est cliente de l'entreprise.

1. L’information est mise en ligne par décision de l’entreprise

Dans la situation ou l’activité est mise en ligne à la suite d’une décision de l’entreprise, celle-ci agissant généralement par le truchement d’un modérateur, c’est l’entreprise (ou l’organisme public) qui assume la responsabilité de ce que comporte les propos mis en ligne émanant du client.

Les contributions peuvent être sous forme de textes écrits, de fichiers sonores, d’images ou de documents vidéo ou encore une combinaison de ces supports. Les contributions peuvent être anonymes ou identifiées. La publication de contributions anonymes peut comporter des risques plus considérables.

2. L’information est mise en ligne par décision d’un tiers

Lorsque c’est un tiers, un client ou une personne qui n’est pas un préposé de l’entreprise qui décide de la mise en ligne, l’entreprise ou l’organisme va se trouver dans la situation d’un intermédiaire. Elle ne prend pas une part active dans la décision de diffuser des informations sur Internet ou encore d’accéder à des informations. C’est le cas, par exemple, lorsque le site de l’entreprise héberge des pages personnelles ou de l’association ou diffuse des commentaires provenant d’internautes. Les entreprises peuvent exploiter des serveurs de courriels ou des listes de discussion. Enfin, il peut s’agir de forums de discussion hébergés dans les installations de l’entreprise. Dans ces situations, les entreprises ou organismes bénéficient de certaines exonérations de responsabilité, c’est-à-dire qu’ils ne sont pas responsables tant et aussi longtemps qu’ils ne jouent qu’un rôle passif dans la diffusion de l’information qui se révélerait illicite et qu’elles n’ont pas connaissance du caractère illicite du propos ou des documents mis en ligne.

III- Les enjeux et risques des principales applications du Web 2.0

Tous ceux qui participent à une activité se déroulant en tout ou en partie sur Internet doivent avoir un comportement prudent. Ils doivent agir comme le ferait une personne normalement prudente et diligente placée en semblables circonstances.

La question est donc celle de savoir ce que constitue un comportement prudent et diligent lorsqu'il s'agit d'activités sur Internet dans les environnements associés au Web 2.0. Cela revient à apprécier les RISQUES associés aux activités et à prendre les PRÉCAUTIONS conséquentes.

Les risques associés à une activité du Web 2.0 ne sont pas tous identiques. Il n'existe pas de recette miracle ou de texte prêt-à-porter qui dispenserait de toute précaution.

Dans la présente partie, l'on explique une MÉTHODE afin d'apprécier les risques et d'identifier les mesures de prudence à observer.

Il s'agit de dégager les critères de bonnes pratiques et les précautions à prendre afin de minimiser les risques.

Ainsi, sont examinés les enjeux et risques associés spécifiquement aux principales applications du Web 2.0. On y examine les principales caractéristiques des différentes familles d'applications qui sont habituellement associées au Web 2.0, l'on explique ce que font les différentes catégories d'acteurs et l'on dresse un tableau des principaux enjeux et risques inhérents au type d'application. Des informations afin d'aider à l'évaluation des risques et une liste des précautions à prendre ou à envisager complètent chacun des chapitres.

A. Les sites de réseaux sociaux

Les sites de réseaux sociaux, nommés *Social Networking Websites* en anglais, offrent des services en ligne qui permettent la rencontre et la mise en relation de différentes personnes. Un grand nombre de sites de réseaux sociaux qui sont aujourd'hui fréquentés par les internautes ont été conçus et développés dans l'environnement juridique américain. Or, aux États-Unis, la loi accorde une très grande immunité à un site Internet qui transmet du matériel émanant d'une autre personne[50]. Plusieurs enjeux et risques à prendre en compte tiennent au fait que l'environnement juridique du Québec présente des différences avec celui qui prévaut aux États-Unis.

---

[50] Molly SACHSON, "The Big Bad Internet: Reassessing Service Provider Immunity under s. 230 to Protect the Private Individual from Unrestrainded Internet Communication", [2011] 25:2 *Journal of Civil Rights & Economic Development* 353-378, http://www.stjohns.edu/academics/graduate/law/journals_activities/jcred/issues/jcred_25_2.stj, visité le 16 décembre 2011.

1. Qu'est-ce qu'un site de réseau social ?

La mise en relation constitue la finalité principale des sites de réseaux sociaux. Un réseau social est orienté vers le Web 2.0, c'est-à-dire que les visiteurs sont des participants actifs du réseau, et non pas de simples visiteurs de pages statiques.

Ces sites de réseautage social ont différentes vocations. Ils peuvent servir à agrandir son cercle d'amis (Facebook), à créer des relations professionnelles (LinkedIn, Viadeo), à faire connaître des groupes musicaux (MySpace), à se mettre en relation avec des gens qui partagent les mêmes intérêts (politiques comme Espoir à Gauche, Néthique, Oliceo; culturels comme Flixster), à retrouver d'anciens camarades de classe (Classmates.com), etc. Il suffit de choisir le site qui répond à nos besoins et de s'y inscrire pour être relié à un ensemble indéterminé de personnes.

Il y a deux façons de se joindre à un site de réseautage social sur Internet. On peut recevoir un courriel de la part d'un ami qui nous invite à s'inscrire sur le site ou encore on peut se rendre directement sur le site de réseautage social qui nous intéresse pour remplir le formulaire d'inscription. Certains sites limitent la croissance de leur réseau en réservant la possibilité de s'inscrire à ceux qui ont reçu une invitation.

Le formulaire d'inscription permet en général de créer un profil de base, qui peut contenir le nom, la ville de résidence ainsi que l'occupation. Par la suite, il est possible de compléter les informations personnelles de façon plus détaillée, en ajoutant une photographie, un curriculum vitae ou encore des centres d'intérêts. Ces renseignements sont regroupés dans un espace personnel.

Pour profiter de la mise en relation avec d'autres personnes, on peut ajouter des contacts à notre carnet d'adresses en recherchant des individus qui sont déjà membres du site et en leur envoyant des demandes de mise en relation. Certains sites vont offrir d'importer la liste contacts d'une adresse de courrier électronique déjà existante dans le but d'envoyer à toutes ces personnes des courriels d'invitation. Si les personnes concernées se joignent au site, elles apporteront à leur tour leurs contacts et le réseau grandit de cette façon.

Une multitude de services sont disponibles sur ces sites. Certains n'offrent qu'un outil de recherche pour rejoindre des individus alors que d'autres offrent de créer un blogue, de mettre en ligne du contenu diffusé en transit, de publier des commentaires, etc. De plus, les sites de réseaux sociaux offrent plusieurs avantages à leurs membres : un sentiment de connectivité et d'intimité plus souvent par rapport à une communauté hors-ligne, mais également face à une nouvelle communauté en ligne. Certains outils permettent aux usagers partageant des points communs de se découvrir mutuellement

et d'interagir. D'autres outils font en sorte que les usagers ont le contrôle sur le contenu qu'ils ont créé (ce qui n'est pas permis par les blogues, par exemple)[51].

a. Qui fait quoi ?

Les réseaux sociaux mettent des personnes en relation. Les usagers y tiennent donc un rôle majeur. Mais les entités qui contribuent à faire des réseaux sociaux de tels environnements assument aussi des obligations et génèrent leur part d'enjeux et de risques.

i) Usagers

L'essence même des réseaux sociaux est la représentation que les personnes peuvent faire d'elles-mêmes et leur mise en relation. Dans ces environnements, les usagers se révèlent, ils publient des informations sur eux-mêmes et sur d'autres ; ils possèdent la faculté de rendre disponibles un vaste ensemble d'informations. En plus, les usagers sont en mesure d'établir des interactions un à un ou des interactions avec un ensemble de personnes.

Les réseaux sociaux fixent l'âge minimal pour devenir membre à 13 ans[52]. Hormis le recours à des modes de vérification en ligne de l'identité qui garantiraient que la personne se trouvant en ligne est effectivement celle qu'elle prétend être, il demeure très difficile d'obtenir une certitude quant à l'âge d'une personne. De plus, il appert que plusieurs approches de vérification de l'âge peuvent comporter plus d'inconvénients que d'avantages, notamment au regard des risques de leurre et d'abus commis à l'endroit de personnes mineures[53].

L'usager qui possède un compte sur un site de réseau social dispose d'espaces privatifs et d'espaces virtuels qui sont accessibles par un ensemble plus ou moins étendu selon les configurations du site ou selon les choix de l'usager. Par exemple, sur Facebook, le profil d'un membre est constitué d'un « mur » comportant une nomenclature d'informations sur l'individu membre, des photos, des liens vers d'autres contenus et autres renseignements indiqués par le membre titulaire du compte. La plateforme génère aussi de façon automatique une liste d'activités récentes en relation avec le compte. Enfin, des tiers peuvent publier des informations qui pourront apparaître sur les pages du titulaire du compte.

---

51 EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY, « Security Issues and Recommendations for Online Social Networks », *ENISA Position Paper n° 1,* Octobre 2007.

52 Voir, clause 4 des Conditions d'utilisation de Facebook, http://www.facebook.com/legal/terms , (visité le 19 décembre 2011).

53 Voir : Adam THIERER, *Social Networking and Age Verification: Many Hard Questions; No Easy Solutions, Progress on Point*, The progress & Freedom Foundation, March 2007, www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf

L'usager peut configurer son compte de façon à rendre accessibles les informations qui s'y trouvent à un cercle plus ou moins étendu. Par exemple, sur Facebook, les paramètres de confidentialité permettent à l'usager de déterminer si les différents types de contenus seront accessibles à tout le monde, uniquement à leurs « amis » ou encore aux amis de leurs amis. Facebook propose aussi l'option de personnaliser les configurations de manière à rendre accessibles ou non certaines catégories d'information, même à l'égard d'un groupe ou de certaines personnes.

ii) « Contacts » et « amis »

Les « contacts » ou « amis » désignent des personnes avec lesquelles un usager entretient une relation plus spécifique. Les relations peuvent être symétriques : par exemple, sur Facebook les relations entre « amis » sont symétriques. Si je suis votre ami, vous êtes nécessairement mon « ami ». D'autres sites de réseaux sociaux permettent d'établir des rapports asymétriques[54]. Le fait d'être en relation dans le contexte d'un réseau social n'est pas, en soi, une preuve de liens d'affection ou d'intimité. C'est tout au plus un indice d'une intention de demeurer en contact avec les personnes faisant partie de la liste que constitue l'usager.

iii) Les « communautés »

Les sites de réseaux sociaux permettent l'établissement de « communautés », c'est-à-dire des ensembles plus ou moins étendus de personnes réunies autour d'intérêts qui peuvent avoir un caractère universel ou encore ne concerner qu'un ensemble restreint d'individus. Des cercles de nature variable se constituent qui partagent des intérêts et des informations. Au sein d'un cercle en particulier, un type d'information peut n'avoir qu'une signification banale alors qu'elle prendra un autre sens, si elle est partagée avec des personnes se trouvant dans d'autres cercles.

Ainsi, les usagers des sites de réseaux sociaux s'inscrivent dans le cadre d'environnements possédant un caractère collectif. Participer à un site de réseau social suppose nécessairement une volonté de partager des informations avec d'autres. Mais ces « autres » participants peuvent se trouver au sein de communautés différentes les unes des autres.

iv) Les développeurs

Outre les usagers et les amis, les développeurs jouent un rôle important. Ces derniers créent de nouvelles applications à partir des données inscrites dans les profils des membres des réseaux sociaux. Ainsi, ils se baseront sur l'activité professionnelle, les contacts et l'activité du profil des membres partout dans le monde.

---

[54] James GRIMMELMAN, « Saving Facebook », [2009] 94 *Iowa L. Rev.,* 1138, p. 1143.

Or, si on se base sur le mode de fonctionnement du réseau Facebook, quand les usagers ajoutent une application (quelle qu'elle soit ; jeu, questionnaire ou petite annonce) à leur page personnelle, ils consentent aussi à ce que les développeurs aient accès à leurs renseignements personnels ainsi qu'à ceux de leurs amis. Dans ces cas, l'unique moyen de refuser une telle communication, lorsque des amis ajoutent une application, est de refuser toutes les applications ou de bloquer des applications particulières[55].

Cela a posé problème pour la Commissaire à la vie privée du Canada qui a recommandé que « Facebook mette en œuvre des mesures techniques pour faire en sorte que les développeurs aient uniquement accès aux renseignements des utilisateurs qui sont essentiels au fonctionnement de l'application »[56]. De plus, la Commissaire a demandé à Facebook de « s'assurer que les utilisateurs sont informés des renseignements précis exigés par l'application, et des fins pour lesquelles on recueille ces renseignements »[57].

v) Les sites de réseaux sociaux

Les sites de réseaux sociaux les plus fréquentés ont été développés aux États-Unis. Dans une grande mesure, leur fonctionnement reflète les traits du droit américain, notamment quant à la place respective que tiennent la liberté d'expression et d'autres intérêts comme le droit à la vie privée. Ainsi, dans la mesure où les informations se trouvant sur les pages d'un site de réseau social émanent des usagers ou de tiers, la législation américaine exclut que les gestionnaires de ces sites puissent être trouvés responsables de ces informations. En Europe, la position du Groupe de travail « Article 29 » sur la protection des données reflète la nette préférence du droit européen pour la protection de la vie privée. Pour ce groupe d'experts de l'Union européenne, les sites de réseaux sociaux « sont responsables du traitement des données conformément à la directive sur la protection des données »[58].

Pour ce qui est du droit québécois, selon la *Loi concernant le cadre juridique des technologies de l'information*, les réseaux sociaux présentent les caractéristiques de prestataires offrant « des services de conservation de documents technologiques sur un réseau de communication » ou encore « des services de référence à des documents

---

55 COMMISSARIAT À LA VIE PRIVÉE DU CANADA, « Facebook doit améliorer ses pratiques en matière de protection de la vie privée, selon les résultats d'une enquête », Communiqués, en ligne : http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_f.cfm (site consulté le 19 décembre 2011).

56 COMMISSARIAT À LA VIE PRIVÉE DU CANADA, « Facebook doit améliorer ses pratiques en matière de protection de la vie privée, selon les résultats d'une enquête », Communiqués, en ligne : http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_f.cfm (site consulté le 19 décembre 2011).

57 COMMISSARIAT À LA VIE PRIVÉE DU CANADA, « Facebook doit améliorer ses pratiques en matière de protection de la vie privée, selon les résultats d'une enquête », Communiqués, en ligne : http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_f.cfm (site consulté le 19 décembre 2011).

58 GROUPE DE TRAVAIL, « Article 29 sur la protection des données », Avis sur les réseaux sociaux en ligne, 19 décembre 2011, http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm, p. 5.

technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche » tels qu'envisagés à l'article 22.

Ainsi qualifiés, ces prestataires ne sont pas tenus à une obligation de surveillance active[59]. La possibilité d'engager leur responsabilité naît lorsqu'il est établi qu'ils ont la connaissance de fait ou la connaissance de circonstances rendant apparente la réalisation d'une activité à caractère illicite sur leur site. La connaissance du caractère délictueux d'un document joue un rôle analogue à l'égard du prestataire agissant à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche.

b. Utilisation des réseaux sociaux

Un site de réseau social, comme Facebook, regroupe des fonctionnalités qui sont propres aux autres médias sociaux. Il permet de communiquer directement avec les autres utilisateurs, par messages privés (semblables au courriel) ou publics (dépendamment des paramètres de confidentialité choisis). Il permet d'opérer un blogue, c'est-à-dire de publier des billets. Également, cet outil sert à publier du contenu multimédia, soit des images, de la musique et des vidéos.

Comme les autres outils du Web 2.0, les entreprises, les organismes publics ou un membre de leur personnel peuvent se créer un compte sur un réseau social comme Facebook.

Une entreprise ou un organisme pourrait se créer une page afin de diffuser le même type d'informations que sur un blogue. Les organisations sont d'ailleurs de plus en plus nombreuses à le faire. Il s'agit d'une façon de communiquer avec la clientèle, notamment en créant des groupes dédiés. Par exemple, les pages Facebook peuvent être publiques, donc facile d'accès pour les clients (au même titre que tout autre site Web).

Quant aux membres du personnel, eux aussi peuvent s'en servir pour communiquer, autant de façon formelle que de façon informelle, à l'intérieur conmme à l'extérieur de l'entreprise.

À l'interne, les réseaux sociaux permettent notamment de développer plus facilement des relations qui pourront déborder en dehors des heures de travail et ainsi améliorer la communication et la cohésion d'une équipe. Ils servent aussi à mettre en place et à bâtir des équipes d'employés qui sont éloignés physiquement. Les employés peuvent définir

59 Art 27 *Loi concernant le cadre juridique des technologies de l'Information*.

clairement, dans leur profil, leurs tâches et leurs projets en cours, favorisant ainsi la communication plus efficace entre employés.[60]

Par exemple, afin de tenter de réduire le recours aux sous-traitants, le géant des services de technologie de l'information EMC avait mis en place une plateforme qui permettait à ses quelque 40 000 employés de s'organiser en réseau et de prendre contact pour la réalisation de leurs projets. L'entreprise avait pris cette initiative car, suite à de nombreuses acquisitions, elle comptait dans ses rangs plusieurs nouveaux employés. Après coup, elle estime que ce projet lui a permis de sauver plus de quarante millions de dollars.[61]

De nos jours, alors que plusieurs entreprises interdisent encore l'utilisation de Facebook et de Twitter au travail, de nombreuses études montrent que l'utilisation de tels espaces virtuels permet de promouvoir des objectifs communs et d'augmenter la confiance. On propose d'utiliser les espaces virtuels pour encourager les rencontres informelles entre employés, en vue de favoriser la coopération et l'innovation au sein de l'entreprise. [62]

À l'externe, grâce aux réseaux sociaux (surtout LinkedIn), les employés peuvent entrer en contact avec d'autres professionnels et ainsi créer des relations d'affaires. Les réseaux sociaux sont utilisés pour donner une visibilité à l'entreprise, une image de proximité et de disponibilité, et ainsi créer des contacts avec des clients potentiels, ou simplement préserver ces contacts avec des clients actuels.

2. Quels sont les risques associés aux sites de réseautage social ?

Les réseaux sociaux offrent des fonctionnalités permettant aux usagers d'interagir et d'organiser leurs interactions. Les usagers doivent effectivement avoir la maîtrise de l'information qui les concerne. En contrepartie, ils doivent être en mesure d'assumer les risques résultant des décisions qu'ils prennent à l'égard des informations qu'ils traitent.

a. La divulgation de renseignements personnels et de renseignements confidentiels

Le risque le plus important, lors de l'utilisation des sites de réseaux sociaux, tient à la facilité avec laquelle il est possible d'y divulguer des renseignements personnels sur soi-même, sur les autres et sur l'entreprise.

---

60 Richard A. PAUL et Lisa HIRD CHUNG, « Brave New Cyberworld : The Employer's Legal Guide To The Interactive Internet » (2008) 24 The Labor Lawyer 109, p. 118.

61 H. James WILSON, PJ GUINAN, Salvatore PARISE et Bruce D. WEINBERG. [2011] "What's Your Social Media Strategy?" *Harvard Business Review* 89 (July-August 2011), p. 24.

62 Paul ADLER, Charles HECKSCHER et Laurence PRUSAK [2011] "Building a Collaborative Enterprise" *Harvard Business Review* 89 (July-August 2011), p. 107.

Par exemple, dans un site de réseau social, il est possible de publier des renseignements nous concernant, mais aussi des renseignements concernant nos contacts. De telles informations peuvent être dévoilées lors de la diffusion d'un commentaire. Nos contacts peuvent également mettre des renseignements nous concernant dans leurs propres sites personnels. Ces sites amènent souvent à dévoiler des coordonnées telles que l'adresse de résidence, les numéros de téléphone et l'adresse de courrier électronique. Les usagers peuvent également y mettre des photographies qui peuvent être interprétées de façon différente par ceux qui y ont accès.

Si plusieurs de ces informations, prises isolément, ont habituellement un caractère anodin, le potentiel pouvant émerger de la combinaison de ces informations avec d'autres renseignements disponibles dans les pages personnelles d'un site de réseau social peut devenir préoccupant car les environnements de réseaux sociaux rendent très facile le jumelage de renseignements relatifs à une personne et, par conséquent, la possibilité de révélation indirecte d'informations personnelles dont certaines pourraient constituer des révélations sur la vie privée. Par exemple, les allusions aux endroits fréquentés ainsi que des informations sur les allées et venues d'un usager ou de ses amis pourraient générer des révélations allant au-delà de ce que la personne concernée par les révélations aurait souhaité partager.

Le participant peut aussi être amené à partager de l'information sur l'entreprise sur les réseaux sociaux. Un employeur qui n'aborde pas l'utilisation de réseaux sociaux dans ses politiques ou dans le contrat d'embauche pourrait se voir confronté à une problématique où l'employé a divulgué des informations confidentielles de l'entreprise, comme les secrets de commerce et des listes de clients.

Questions à vérifier

- *Le participant est-il amené à dévoiler des renseignements personnels et confidentiels sur lui-même ou sur une autre personne (et sur l'entreprise/organisme public) ?*
- *Le participant est-il au courant des risques inhérents à l'utilisation de cet outil ?*
- *Est-ce qu'il y a un contrôle sur l'âge des participants ?*
- *Le site de réseau social offre-t-il différents paramètres qui permettent au participant de décider à quel point il partage ses informations personnelles, et avec qui ?*
- *Les politiques de l'entreprise/organisme déterminent-elles la confidentialité de certaines informations de l'entreprise (exemple : les listes de contacts-clients), à qui elles appartiennent, et ce qui arrive avec celles-ci en cas de terminaison d'emploi ?*
- *A-t-on informé les employés sur la confidentialité de ces informations, ou mis en place des mesures de protection qui les amèneraient à conclure que ces informations sont confidentielles ?*
- *Les politiques de l'entreprise/organisme indiquent-elles dans quels cas l'employeur s'autorise à faire du monitoring des activités de l'employé sur les réseaux sociaux ?*

b. Les rencontres hors-ligne avec des étrangers

Il est possible de vouloir prendre contact dans la réalité avec une personne faisant partie de notre réseau social. C'est d'ailleurs un excellent moyen de rencontrer d'autres professionnels et de développer un réseau pour de potentielles relations d'affaires. Ces rencontres peuvent toutefois être risquées puisqu'il est possible pour un individu de se faire passer pour quelqu'un d'autre sur ces sites.

Questions à vérifier

- *Le site offre-t-il la possibilité de communiquer de façon privée ?*
- *Le participant est-il amené à dévoiler des renseignements personnels sur lui-même ou sur une autre personne (et sur l'entreprise/organisme public) ?*
- *Le participant s'est-il assuré de la crédibilité des informations présentées par les étrangers avant de les rencontrer? La rencontre aura-t-elle lieu en public ?*

c. L'utilisation non autorisée de l'image, de la marque, et les atteintes au droit d'auteur

Sur les sites de réseaux sociaux, il y a un risque d'atteinte au droit d'auteur et aux autres droits sur des informations identifiant les individus ou les organisations. Certains sites offrent de partager du contenu à l'intérieur des espaces personnels. Par exemple, un individu pourrait publier des vidéos contenant des sketches d'un humoriste sans son consentement. Cette diffusion de contenu peut donc constituer une atteinte au droit d'auteur de l'artiste.

Les sites de réseaux sociaux permettent de diffuser des images de personnes, des signes distinctifs, des marques de commerce ou des images d'objets. Les enjeux relatifs à la diffusion des images concernent évidemment les droits de propriété intellectuelle pouvant exister sur celles-ci mais ils mettent aussi en jeu le droit des personnes de s'opposer à la diffusion de leur image sans leur consentement ou en dehors de circonstances où la diffusion serait justifiée par l'intérêt public ou par l'intérêt que pourraient avoir certains proches. Par exemple, utiliser des photographies de nos contacts au sein d'un album en ligne peut constituer une atteinte au droit à l'image d'une personne, lorsqu'elle est faite sans son consentement.

Alors qu'en droit américain, on peut déduire le consentement implicite suite à l'utilisation de la fonction « *tagging* », cela est beaucoup moins certain en droit québécois où le droit à l'image jouit d'une protection beaucoup plus forte[63] On peut penser aux situations problématiques causées par des photos de cocktails ou 5 à 7 mises en ligne par des entreprises/organismes publics. La diffusion non autorisée de signes

---

[63] Valentin CALLIPEL, « Faut-il obtenir le consentement d'un individu que l'on "tag" sur facebook ? », Chaire en droit de la sécurité et des affaires électroniques, Université de Montréal, 5 avril 2011, http://www.gautrais.com/Faut-il-obtenir-le-consentement-d (visité le 19 décembre 2011).

distinctifs et marques de commerce constitue aussi un risque qui doit être soigneusement évalué.

> ***Questions à vérifier***
> - *Est-ce que le contenu contient des œuvres ou parties d'œuvres qui sont protégées par la* Loi sur le droit d'auteur *?*
> - *Est-ce que la personne qui diffuse l'information détient les autorisations nécessaires pour la publier ?*
> - *Est-il possible de garder une copie des documents audio ou vidéo ? Internet regorge d'outils permettant d'intercepter et d'enregistrer un flux de sons ou d'images pour les divers formats utilisés.*
> - *Est-ce que le contenu visionné (et le contenu mis en ligne…) contient des images de personnes identifiables ?*

d. Les contenus à caractère pornographique

Il est possible de trouver des images à caractère pornographique dans les espaces personnels des personnes qui sont inscrites à des sites de réseautage social. Ce contenu, quoique généralement interdit dans les conditions d'utilisation de ces sites, peut ne pas convenir à certains publics et peuvent affecter négativement la réputation des entités impliquées. Lorsqu'un tel contenu est dénoncé, les administrateurs du site retirent habituellement le contenu en question, ou encore ferment le compte de la personne fautive. Certains sites de réseaux sociaux proposent un service exclusivement destiné aux adultes.

> ***Questions à vérifier***
> - *Quelles sont les précautions prises pour limiter l'accès à des documents qui ne sont pas appropriés ?*
> - *Quel est le public visé ? Le contenu est-il approprié pour ce public ? Le public sur Internet est souvent plus large que ce qui est visé (exemple : sur Facebook, un lien publié par une personne X peut être visionné par une personne Z non liée, par l'entremise d'une personne Y.)*

e. Les atteintes à la réputation, la propagande haineuse, le harcèlement et les menaces

Vu la quantité et la diversité des informations que l'on peut retrouver sur les sites de réseautage social, des personnes mal intentionnées peuvent se servir de ces renseignements dans un but illicite, par exemple, en ciblant quelqu'un pour lui envoyer des menaces ou écrire des propos haineux ou diffamants par rapport à cette personne ou à un groupe de personnes[64].

---

[64] Voir Tristan PÉLOQUIN, « Six élèves suspendus pour un site Web diffamatoire », *La Presse*, 16 mai 2007, p. A8

Une personne peut également produire un profil sur une autre personne et publier des messages diffamatoires ou encore des informations mensongères. De même, le contenu publié sur le site peut être réutilisé à mauvais escient par des personnes. Par exemple, si quelqu'un envoie une photographie osée à un contact ou la met en ligne, le contact peut s'en servir ensuite pour harceler la personne en question. Il peut la menacer d'envoyer la photographie à des proches, dans le but de salir sa réputation ou d'obtenir d'autres photographies d'elle.

Un employé qui dénigre un compétiteur sur les réseaux sociaux pourrait engager la responsabilité de son employeur, si le propos est diffusé dans un contexte présentant un lien de connexité avec les activités de ce dernier.

Questions à vérifier

- *A-t-on sensibilisé l'employé au fait que son comportement en ligne doit être impeccablement conforme aux politiques de l'entreprise et ce, même en utilisant le matériel à son domicile ?*
- *Est-ce que les faits présentés sur les espaces personnels sont vérifiés et vérifiables ? Il peut y avoir diffamation, même si les informations sont vraies[65]. Pour certaines informations, leur révélation doit être dans l'intérêt public et non pas dans le seul but de nuire. Exemple : écrire sur le « mur » de quelqu'un qu'il est homosexuel, même si c'est vrai et théoriquement sans offense, pourrait constituer de la diffamation ou une violation de la vie privée.*
- *Est-ce qu'il y a présence de surveillance sur le site ? (et des moyens d'effacer l'information publiée par les autres et par nous-mêmes sur notre profil ?)*
- *Quel est le sujet traité sur l'espace personnel ? Sur les espaces publics ? Quel contenu y retrouve-t-on ?*
- *Sommes-nous appelés à révéler des renseignements personnels sur notre espace personnel ? Dans les espaces partagés ?*

f. L'utilisation décontextualisée des renseignements personnels

Les possibilités d'utilisation des renseignements personnels dans un contexte différent de celui dans lequel ils ont été initialement partagés constituent un autre ensemble de risques. Les informations personnelles dévoilées sur un site de réseau social peuvent être utilisées de plusieurs façons. Par exemple, des entreprises peuvent se servir des informations pour sonder le marché, des prédateurs sexuels peuvent trouver des victimes potentielles, en recherchant des profils vulnérables, ou des employeurs éventuels peuvent surfer sur les espaces personnels pour en apprendre plus sur des candidats avant de les engager.

g. Le risque de falsification d'identité

Un utilisateur peut créer un faux profil afin de nuire à une autre personne ou de faire une blague. Par exemple, un candidat à un poste pourrait créer un profil défavorable au

---

65 http://www.barreau.qc.ca/publications/journal/vol34/no15/procedures.html

nom d'un compétiteur afin de miner ses chances et ainsi augmenter les siennes. Au Royaume-Uni, Grant Raphael a été reconnu coupable d'atteinte à la vie privée et de diffamation pour avoir publié de fausses informations sur un ancien collègue d'école, Mathew Firsht, via un faux profil (notamment sur son orientation sexuelle et ses opinions politiques, ainsi que des allégations concernant des dettes de sa compagnie, mettant en doute la fiabilité de celle-ci)[66].

Pour faire la promotion d'une biographie non autorisée sur Guy Laliberté, l'auteur de la biographie et son éditeur ont mis en ligne une page MySpace au nom de Monsieur Laliberté, usurpant ainsi son identité et trompant les internautes. La Cour supérieure du Québec conclut à la violation de la vie privée du demandeur Laliberté et indique qu'« il s'agit clairement d'une violation de la vie privée. Il n'y a aucune légitimité à emprunter l'identité d'une personne pour laisser croire qu'il est le destinataire de la correspondance qui lui est adressée et qu'il est l'auteur des réponses qui y sont données »[67].

Question à vérifier
- *Le site offre-t-il la possibilité de dénoncer les faux profils ?*

h. Le risque de vol d'information personnelle, vol d'identité, sollicitation indésirable

Sur les sites de réseaux sociaux, les gens révèlent beaucoup d'information sur eux-mêmes, sans être nécessairement conscients de qui peut avoir accès à leur profil et des options de confidentialité disponibles. Certains risques découlent de la facilité d'accès aux profils personnels sur les sites de réseautage social et des possibilités de référencement[68] (*data mining* et *spidering*) et d'hameçonnage[69] (*phishing*) qui sont susceptibles de survenir.

Plusieurs des fonctions des réseaux sociaux peuvent être détournées afin de harceler d'autres personnes. Par exemple, les fonctions de messageries peuvent être utilisées afin d'interagir directement avec une personne. L'affichage d'informations peut aussi servir à harceler une autre personne.

Les questions usuelles de sécurité (nom, adresse, nom de son animal de compagnie, nom de jeune fille de sa mère...) peuvent souvent trouver réponse dans une page

---

66 « Payout for False Facebook Profile », *BBC News*, 24 juillet 2008, en ligne : http://news.bbc.co.uk/2/hi/7523128.stm (site consulté le 19 décembre 2011).

67 *Laliberté* c. *Transit Éditeur inc.*, 2009 QCCS 6177 (CanLII), par. 30.

68 Wikipédia, « Robot d'indexation », en ligne : fr.wikipedia.org/wiki/Robot_d%27indexation (site consulté le 19 décembre 2011).

69 Wikipédia, « Hameçonnage », en ligne : fr.wikipedia.org/wiki/Hameconnage (site consulté le 19 décembre 2011).

Facebook. Or malgré les consignes de sécurité, plusieurs personnes utilisent des informations personnelles pour générer leurs mots de passe, ce qui facilite le travail de fraudeurs.

Une entreprise ou un organisme doit sensibiliser ses employés aux risques du référencement (*data mining/spidering*) et du hameçonnage (*phishing)* afin de s'en protéger.

i. L'utilisation des sites de réseautage à des fins judiciaires ou disciplinaires

Les informations consignées dans les environnements des réseaux sociaux sont susceptibles d'être utilisées dans le cadre de procédures devant les tribunaux ou devant des instances disciplinaires[70]. L'usager aura beau configurer son profil de façon à ne réserver qu'à des « amis » triés sur le volet l'accès à certaines informations, il lui est impossible d'exclure le droit d'autres entités d'avoir accès à ces informations, notamment dans le cadre de litiges devant les tribunaux.

Le pouvoir des tribunaux d'ordonner la production de contenus, même privés, sur les réseaux sociaux constitue le principal risque de régulation découlant des activités des réseaux sociaux. Ainsi, les photos et propos publiés sur les sites de réseaux sociaux sont souvent utilisés en preuve pour constater des méfaits, que ce soit la consommation d'alcool, l'identification de manifestants ou la brutalité policière. Ces informations sont régulièrement mises en preuve pour trancher l'attribution de la garde des enfants.

Les sites sont également utilisés pour justifier des mesures disciplinaires, notamment envers des personnes ayant diffusé des propos incendiaires à l'égard de membres de la direction, ou envers des employés aux « cyber-comportements » discutables. Il devient alors parfois difficile de mettre en balance la liberté d'expression, d'une part, et le droit au respect de l'image, de la vie privée et de la réputation, d'autre part.

Question à vérifier

- *Le participant est-il conscient que ce qu'il écrit et partage, même en privé, peut être utilisé à des fins judiciaires ?*

j. La persistance de l'information

La possibilité, pour l'usager, de supprimer complètement son compte peut poser des difficultés. Ainsi, pendant les premières années de mise en service, il était pratiquement impossible de supprimer son compte Facebook. En effet seule la désactivation était possible jusqu'à récemment. Il est maintenant possible de supprimer complètement son

70 Nicolas W. VERMEYS, « L'admissibilité en preuve de contenus issus de sites de réseaux sociaux », *Repères*, Juillet 2010, EYB2010REP962; Pamela D. PENGELLEY, *Fessing Up to Facebook: Recent Trends in the Use of Social Network Websites for Insurance Litigation,* March 3, 2009, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1352670.

compte : les informations ne pourront plus être retrouvées si la personne décide de s'ouvrir un compte de nouveau. Or, même en supprimant son profil, il est impossible de savoir si Facebook conserve effectivement ces données sur ses serveurs et, si oui, à quelles fins et pour combien de temps.

Les participants doivent être conscients du caractère permanent des informations mises en ligne, et de la possibilité pour tous ceux qui y ont accès d'en prendre une copie ou capture d'écran et de les partager par la suite.

3. Comment évaluer ces risques ?

a. Les comportements et les caractéristiques des usagers

Dans les réseaux sociaux, plusieurs risques découlent principalement des comportements adoptés par les internautes. On se retrouve donc avec une multitude de centres de décision, tous en mesure de diffuser des informations à partir de leurs propres perspectives. Ce rôle accru des individus « amateurs », dans des situations autrefois dominées par des professionnels, tend à brouiller les frontières entre producteur et consommateur, ce qui dramatise la question des statuts et responsabilités respectives des uns et des autres[71].

Questions à vérifier

- *Quel est le public visé par le site de réseautage social ?*
- *Est-ce que l'on retrouve du contenu qui pourrait être inapproprié pour le public visé sur le site de réseautage social ?*
- *A-t-on mis en place des modes de formation des employés à l'utilisation raisonnable et attendue par l'entreprise/organisme du Web 2.0 dans le cadre de l'emploi ?*

b. Les services offerts par le site de réseau social

Le niveau de risque sur un site de réseau social variera en fonction des services offerts. Un site proposant simplement un moyen de mettre en relation des personnes présentera nécessairement moins de risque qu'un autre offrant des fonctions de partage de contenu, de blogue et de messagerie instantanée. Les développements d'applications peuvent être une source de risque parce qu'elles impliquent souvent le dévoilement d'information sur les usagers. Elles peuvent amener aussi des actions sur le réseau social à partir du profil l'utilisateur qui n'a pas nécessairement consenti.

---

71 Pierre-Yves GAUTIER, « Le contenu généré par l'utilisateur », *LÉGICOM*, n° 41, 2008/1, p. 1-7.

> ***Question à vérifier***
> - *Est-ce qu'il y a présence de sons, d'images ou de vidéos sur le site de réseau social ? Si oui, est-ce que l'usager détient les autorisations nécessaires pour les utiliser ?*
> - *Le site de réseau social permet-il le développement d'application*

c. La présence de surveillance sur le site

Il est possible qu'un site exerce une vérification aléatoire de son contenu. Lorsqu'un contenu inapproprié est découvert de cette façon, les administrateurs devront prendre des moyens pour le retirer. Les tribunaux québécois n'ont pas encore tranché la question à savoir si un site qui exerce une vérification aléatoire sur son contenu peut en être tenu responsable. Il convient donc de faire preuve de prudence en optant pour cette façon de faire, en particulier s'il est impossible de vérifier tout le contenu du site vu son ampleur.

> ***Questions à vérifier***
> - *Les administrateurs du site exercent-ils une vérification sur le contenu publié ?*
> - *Quelles sont les conséquences lorsqu'une personne publie du matériel inapproprié ?*

d. La présence d'un moyen de dénoncer le contenu inapproprié

Certains sites ou environnements proposent aux usagers un moyen de dénoncer un espace personnel au contenu inapproprié. Cette façon de faire est généralement efficace puisque les administrateurs du site seuls ne peuvent surveiller tout le contenu qui est hébergé. De plus, une telle pratique incite les gens à ne pas publier de matériel offensant puisqu'ils ont plus de risque de se faire dénoncer.

> ***Question à vérifier***
> - *Est-ce qu'il y a une procédure de vérification par les tiers du contenu sur le site ? Si oui, cette procédure est-elle facile d'utilisation ?*

4. Quelles sont les précautions à prendre ?

La grande liberté dont dispose l'usager dans les sites de réseaux sociaux fait en sorte qu'il lui incombe de prendre les précautions qui sont appropriées aux risques qu'il accepte de courir dans ces environnements.

a. Éviter de mettre en ligne des renseignements personnels

Lors de l'inscription à un site de réseau social, il faut éviter de donner des renseignements personnels comme son nom et son prénom, son adresse, ou sa date de naissance. Il faut également s'abstenir de fournir son numéro de carte d'assurance-maladie, d'assurance sociale, ou encore de carte bancaire. Des renseignements à première vue anodins, comme nos endroits préférés de sortie, peuvent aussi être utilisés à mauvais escient.

De plus, il faut faire attention aux messages publiés dans son profil ou dans celui de ses contacts puisque des informations personnelles peuvent s'y glisser. Il peut être avisé de naviguer régulièrement sur les profils de ses différents amis pour vérifier qu'aucun renseignement nous concernant n'y soit inscrit.

Il faut aussi s'abstenir de publier sur un tel site des propos ou des photos susceptibles de nuire à des proches, ainsi que des propos mensongers ou diffamants, et ce, même si les paramètres de confidentialité sont élevés.

Il peut être également utile de vérifier qu'il n'y a rien d'indésirable ou de mensonger à son sujet sur le Web (ou au sujet d'un homonyme), par exemple, en étant à l'affût des photos compromettantes qui pourraient être diffusées par des amis ou des connaissances. En effet, toute information qui se retrouve sur un site de réseautage social est susceptible d'être lue par le grand public.

b. Mettre en place un haut degré de protection de notre profil et éviter le contact avec des inconnus

Les sites de réseautage social mettent habituellement à la disposition des utilisateurs une page où il est possible de changer les paramètres de sécurité de son profil. Les usagers peuvent donc afficher leur profil comme étant privé, ce qui permet seulement à leurs amis de les voir, ou encore ils peuvent bloquer certaines fonctions comme la possibilité de laisser des commentaires ou d'utiliser la messagerie instantanée.

Il est important, pour plus de sécurité, de choisir un site de réseautage qui offre la possibilité d'ajuster ces paramètres. De plus, lorsque cette fonction est disponible, les utilisateurs du service devraient appliquer le plus haut degré de protection possible à leur profil.

Pour une plus grande sécurité, refuser d'entrer en contact avec des gens que l'on ne connaît pas dans la « vraie » vie est une précaution fondamentale, mais qui n'est pas toujours infaillible.

c. Mettre en ligne une procédure de dénonciation

Une procédure de vérification du site par les utilisateurs peut être très utile pour contrôler le contenu d'un site de réseautage social. Il s'agit d'inviter les usagers à dénoncer un contenu illicite, par une méthode facile offerte par le site. En plus de disposer d'un plus grand nombre de vérificateurs - puisque tous les visiteurs peuvent dénoncer un profil - cette méthode n'engagera généralement pas la responsabilité du site, à moins que celui-ci ait été averti du caractère illicite d'un contenu et qu'il ne l'ait pas promptement retiré.

d. **Informer les participants des risques liés à l'usage des sites de réseautage social**

L'usager doit s'informer des dangers liés à l'utilisation d'un site de réseau social. Ces informations devraient d'ailleurs être disponibles sur le site pour consultation par les usagers.

On doit également être informé que tout usager qui rend disponible une œuvre sur un site de réseautage social perd son exclusivité sur ses droits d'auteur. Il faut aussi éviter de publier des œuvres pour lesquelles on ne possède pas les droits, sinon notre responsabilité pourrait être engagée.

B. Les sites de partage de contenu

1. Qu'est-ce qu'un site de partage de contenu ?

Un site de partage de contenu est un site Web où les visiteurs ont la possibilité de mettre en ligne des fichiers, que ce soit des vidéos, des chansons, des livres, etc. En général, ces sites utiliseront la lecture en transit pour diffuser le contenu. Pour visionner un film, par exemple, il suffit d'aller sur un site Internet qui offre ce service, de sélectionner le film, et de l'écouter, sans besoin de l'enregistrer sur un disque dur.

La lecture en transit (*streaming*) est une méthode de diffusion de fichiers audio ou vidéo qui permet leur lecture en temps réel, c'est-à-dire dès le début de la réception du fichier, sans avoir à attendre qu'il soit copié au complet sur l'ordinateur récepteur. Le transfert de données se fait sous forme de flux régulier et continu. La lecture en transit permet donc de diffuser des contenus multimédias sur Internet, à la demande ou en temps réel, et ce, sans solliciter l'espace du disque dur de l'utilisateur.

Les applications de cette technique sont nombreuses : radio et télévision sur Internet, vidéo à la demande, informations audiovisuelles en continu… Pour les compagnies de disques, il s'agit là d'une alternative aux fichiers MP3. Elles peuvent faire valoir leurs produits sans risquer de les faire copier puisqu'il n'y a pas, en principe, de copie durable du fichier transféré.

Les sites les plus connus de partage de contenu sont sans aucun doute YouTube (http://www.youtube.com/) et Dailymotion (http://www.dailymotion.com/). Les visiteurs de tels sites peuvent y publier des films, des vidéoclips, des émissions, etc. Ils peuvent aussi visionner le contenu que d'autres visiteurs ont publié. Les sites de réseaux sociaux sont également utilisés pour partager du contenu puisque certains hébergeurs d'espaces personnels offrent, la possibilité aux membres, par exemple, de mettre en ligne leur musique préférée.

Les sites de partage de contenu offrent en général la possibilité aux visiteurs de laisser des commentaires suite au visionnement de la vidéo ou à l'écoute de la chanson. Il est

aussi possible d'évaluer le document en lui accordant une note, généralement sur cinq (exemple : quatre étoiles sur cinq). Ce système de notation permet de faire une recherche sur le site par rapport au contenu le mieux coté.

Ces sites sont très intéressants pour ceux qui désirent publier du contenu puisque le service est habituellement gratuit. Les coûts de bande passante seront moindres en publiant des vidéos sur YouTube, par exemple, au lieu de les mettre directement sur une page Web personnelle. Il est possible par la suite d'incorporer la vidéo (*embedding*) directement sur le site personnel. De plus, la publication ne demande aucune connaissance particulière en informatique.

a. Qui fait quoi ?

i) Les usagers

La personne qui consulte un site de partage de contenu peut jouer deux rôles.

Il peut être ***visiteur***. Il peut naviguer sur le site pour chercher une vidéo ou un film. Une fois le contenu téléchargé ou visionné, il est souvent amené à l'évaluer et à le commenter.

Il peut également être un ***participant actif.*** Il mettra alors des éléments (vidéos, images, films) sur le site de partage de contenu. Dans le cadre de sites de poste-à-poste, il participera activement, comme client et comme serveur.

ii) Les hébergeurs

Les hébergeurs créent l'architecture informatique permettant à l'utilisateur de téléverser et, ensuite, de visionner le contenu. Ils mettent en place des mécanismes automatiques qui convertissent le contenu dans un format uniforme, lisible par tous les visiteurs. Ce sont aussi eux qui décident de garder ou de retirer un contenu, lorsque celui-ci fait l'objet d'un blâme (*flag*).

Les hébergeurs doivent agir rapidement lorsqu'une vidéo illicite diffusée sur leur site leur est signalée, mais il est difficile de les tenir responsables lorsqu'ils n'ont pas connaissance du caractère illicite des contenus. La tâche de visionnement préalable semble impensable pour un site comme YouTube, considérant la quantité phénoménale de vidéos mises en ligne[72].

---

72 Ryan JUNEE, « Zoinks! 20 Hours of Video Uploaded Every Minute! », YouTube, 20 mai 2009, en ligne: http://www.youtube.com/blog?entry=on4EmafA5MA (site consulté le 19 décembre 2011).

iii) La communauté

On désigne par « communauté » l'ensemble des usagers qui consultent, évaluent et commentent le contenu d'un site. Elle occupe une place importante dans le fonctionnement des sites de partage de contenu. Le nombre de consultations, la note globale et le nombre de commentaires déterminent ensuite la présentation du contenu sur le site. Par exemple, dans une recherche effectuée sur YouTube, les « meilleures » vidéos, selon ces critères, apparaîtront en premier sur le site.

b. Utilisation des sites de partage de contenu

Les sites de partage de contenu permettent d'offrir des activités de formation en ligne. Certaines entreprises mettent des vidéos en ligne pour diffuser des informations et ainsi aider les membres de leur personnel ou leurs clients. Des campagnes publicitaires ont aussi lieu au moyen de sites de partage (ex : AXE). Les organismes publics peuvent aussi s'en servir comme tribune (exemple : aux États-Unis, la Maison Blanche a son propre YouTube *channel*).

À l'interne, YouTube est utile afin mettre en ligne des présentations et vidéos de formation offerts aux employés. Il est possible de créer un « *channel* » privé et permettre aux employés d'accéder et de contribuer au contenu par la publication de commentaires et de questions.

2. Quels sont les risques associés aux sites de partage de contenu ?

Les risques associés aux sites de partage de contenu sont semblables à ceux reliés aux sites de réseaux sociaux. D'ailleurs, plusieurs sites de réseaux sociaux offrent également un service de partage de contenu afin de partager, avec ses contacts, de la musique ou encore des films.

a. L'utilisation non autorisée de l'image et de renseignements personnels

Du contenu de nature personnelle ou relevant du cercle intime d'une personne peut se retrouver sur des sites de partage de contenu, tels des vidéos de fêtes ou encore de sorties entre amis. Ces vidéos peuvent brimer le droit à l'image de quelqu'un s'il est possible d'identifier la personne filmée. Il n'est même pas nécessaire d'utiliser l'image réelle de cette personne pour transgresser ses droits. En effet, l'utilisation d'un sosie dans une vidéo et la mention du nom de la personne imitée peuvent suffire à violer le droit à l'image.

Il faut donc s'assurer, avant de publier une vidéo sur Internet, d'avoir les autorisations nécessaires des personnes qui s'y retrouvent, ou qui y sont représentées. Le même raisonnement s'applique pour les autres types de contenus, par exemple pour les images qui pourraient être mises en ligne.

De plus, puisque les sites de partage de contenu demandent souvent d'inscrire une adresse de courrier électronique pour pouvoir, par exemple, publier un commentaire, il est possible que ce renseignement personnel soit utilisé pour une autre finalité, par exemple pour une liste de diffusion de pourriels. Il est aussi difficile de connaître la persistance des données personnelles et qui sont les tiers ayant accès à ces informations.

Questions à vérifier
• *Est-ce que le contenu visionné contient des images de personnes identifiables ?*
• *Est-ce que l'auteur du contenu détient les autorisations nécessaires pour le publier ?*
• *Est-ce que le site demande l'inscription d'une adresse de courriel ? Est-ce que l'adresse est diffusée sur le site ?*

b. Les contenus haineux, menaçants, diffamatoires et contraires aux lois

Les populaires sites de partage de contenu sont des espaces de choix pour partager des idées et des opinions avec un grand nombre de personnes. Toutefois, ils peuvent devenir des espaces de diffusion de contenus contraires à la loi ou ne convenant pas à certains publics. Les comportements illégaux dans la « vie réelle » le demeurent sur Internet, que ce soit la propagande haineuse, la diffamation, le harcèlement, les menaces ou l'intimidation.

Les actions « virtuelles » confèrent un certain sentiment d'anonymat et d'impunité. De plus, il est difficile d'identifier les responsables. Il y a également un délai entre le moment où la vidéo est mise en ligne, le moment de son signalement comme étant inapproprié (*flagging*) et finalement le moment de son retrait. La vidéo peut donc être vue par un plus grand nombre de personnes et causer davantage de dommages.

Les sites de partage de contenu sont aussi souvent un moyen pour diffuser des vidéos d'agressions physiques, ou *happy slapping*[73]. Ces vidéos, où l'on voit une personne en train de se faire agresser par surprise et de façon tout à fait gratuite, ne sont pas encore interdites spécifiquement dans une loi au Canada. Par contre, la responsabilité des gens qui filment et publient de telles agressions peut être retenue de plusieurs autres façons. Par exemple, ils peuvent être poursuivis pour ne pas avoir porté secours à une personne en péril, obligation qui est prévue à l'article 2 de la *Charte des droits et libertés de la personne*[74]. Il est à noter que certains pays, comme la France[75], ont adopté des lois qui interdisent le *happy slapping* sous peine de se voir attribuer une amende et une peine d'emprisonnement.

---

73 INTERNATIONAL HERALD TRIBUNE, « Le côté sombre des sites de partage de contenu », dans *Canoë*, http://www2.canoe.com/techno/nouvelles/archives/2007/03/20070302-105546.html

74 L.R.Q., c. C-12.

75 *Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance*, J.O. 7 mars 2007, p. 4297, art. 44.

Bien qu'elles ne soient pas illégales en soi, les images sexuellement explicites sont contractuellement interdites sur YouTube. Toutefois, comme la censure du site ne fonctionne pas par choix éditorial préalable, les usagers peuvent se retrouver exposés à de la pornographie et à d'autres contenus inappropriés. Lorsqu'un visiteur signale aux administrateurs d'un site de partage la présence de tels contenus, certains conservent ou retirent simplement le contenu, d'autres l'assortissent d'un avertissement de contenu explicite.

Questions à vérifier

- *Quelles sont les précautions prises pour limiter l'accès à des documents qui ne sont pas appropriés pour certains publics ?*
- *Quel est le public visé ? Le contenu est-il approprié pour ce public ?*
- *Est-ce que les interventions anonymes sont permises sur le site ?*
- *Le site demande-t-il la divulgation de renseignements personnels ?*
- *Est-ce qu'il y a un mécanisme de dénonciation de propos illicites sur le site Web?*
- *A-t-on sensibilisé et formé l'employé au fait que son comportement en ligne doit être en tout point conforme aux politiques de l'entreprise, et ce, même en utilisant le matériel à la maison ?*

c. Les atteintes au droit d'auteur ou aux marques de commerce

Le risque le plus important sur de tels sites est sans doute celui d'utiliser du contenu protégé par le droit d'auteur ou l'utilisation non autorisée de marques de commerce ou autres signes distinctifs.

En droit d'auteur canadien, que ce soit la diffusion en transit d'une chanson, d'un vidéoclip ou d'un livre, même si une œuvre ne se retrouve jamais au complet dans la mémoire Ram de l'usager et que seul d'infimes parties s'y croisent, tour à tour, pour s'effacer lorsque la partie suivante arrive, il s'agit là, strictement parlant, d'une reproduction. En dehors des cas où un détenteur des droits d'auteur propose des œuvres par ce moyen, cette technique pourrait être considérée comme une source illicite de reproduction des œuvres.

Plusieurs situations violant le droit d'auteur peuvent se produire sur les sites de partage de contenu. Par exemple, publier une vidéo dans laquelle il y a un extrait d'une autre vidéo peut conduire à des poursuites de la part de l'auteur de l'extrait[76]. De plus, mettre en ligne une vidéo de notre enfant où l'on utiliserait comme musique de fond une chanson qui est la propriété de quelqu'un d'autre est aussi une atteinte au droit

[76] Sur les faits et non sur le fond, voir : *Doe* v. *Geller*, 533 F.Supp.2d 996 (N.D. Cal. 2008)

d'auteur[77]. Il y a également la situation plus évidente où l'on met directement en ligne une œuvre qui ne nous appartient pas[78].

L'entreprise ou l'organisme public voudra peut-être utiliser YouTube pour faire circuler son message et, ainsi, mettre en ligne des documents qui pourraient être protégés par le droit d'auteur.

De plus, l'entreprise pourrait sanctionner un de ses employés qui partagerait des documents/œuvres protégées ou marques de l'entreprise ou d'un tiers sur les sites de partage.

Questions à vérifier

- *Est-ce que le contenu contient des œuvres ou parties d'œuvres qui sont protégées par la* Loi sur le droit d'auteur *?*
- *Est-ce que la personne qui diffuse l'information détient les autorisations nécessaires pour la publier ?*
- *Quels types d'œuvres sont visionnés ou écoutés ? (ou publiées sur le compte de l'entreprise…)*
- *Est-il possible de garder une copie des documents audio ou vidéo ? Internet regorge d'outils permettant d'intercepter et d'enregistrer un flux de sons ou d'images pour les divers formats utilisés.*
- *Pour du matériel publié par l'entreprise/organisme, a-t-on réellement besoin de garder un contrôle rigoureux sur le droit d'auteur, ou peut-on permettre la réutilisation par des tiers (exemple : à des fins non commerciales) ? Dans le deuxième cas, a-t-on considéré l'utilisation des licences libres ?*

d. La responsabilité pour les informations diffusées

En général, les auteurs seront les premiers responsables de l'information qu'ils publient lorsqu'ils sont identifiés. Si le matériel a été mis en ligne par un employé agissant dans le cadre de ses fonctions au sein de l'entreprise ou de l'organisme public, la responsabilité de l'employeur pourrait être engagée. Les sites eux-mêmes n'ont pas d'obligation de surveiller les documents déposés par les usagers. Par contre, s'ils sont avertis qu'un propos ou document illicite se retrouve sur le site, ils ont l'obligation de réagir et de le retirer si le contenu est effectivement illicite[79].

Questions à vérifier

- *Les interventions anonymes sont-elles permises ?*
- *Est-ce qu'il y a des mécanismes de surveillance du contenu sur le site en question ?*

---

77 Sur les faits et non sur le fond, voir : *Lenz* v. *Universal Music Corp.*, 2008 WL 962102 (N.D. Cal. 2008)

78 Sur les faits et non sur le fond, voir : *Viacom Intern. Inc.* v. *YouTube, Inc.*, 2008 WL 629951 (S.D. N.Y. 2008) ; *Jean-Yves Lafesse et autres / Dailymotion et autres*, Tribunal de grande instance de Paris, 3[e] chambre, 1[e] section, jugement du 15 avril 2008

79 *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 22.

e. L'utilisation des sites de partage de contenu à des fins judiciaires ou disciplinaires

Sur les sites de partage de contenu, les gens diffusent des images et vidéos d'eux-mêmes et de leurs proches. Or, les vidéos publiées peuvent être utilisées en preuve et incriminer les personnes qui commettent les délits qui ont été filmés. Aussi, les vidéos pourraient éventuellement être consultées par des employeurs ou professeurs et conduire à des mesures disciplinaires. L'enjeu n'est toutefois pas aussi présent que pour les sites de réseaux sociaux, où l'identité des personnes est plus directement dévoilée.

Par exemple, une vidéo prise sur la scène du délit par un observateur a été mise en ligne sur YouTube et a servi de preuve lors du procès[80]. Également, une vidéo diffusée sur YouTube montrant un graffitiste californien à l'œuvre sur le muret d'un viaduc a servi de preuve incriminante lors de son procès pour vandalisme[81].

Dans une affaire survenue en 2008[82], deux adolescents ont été condamnés, suite à l'enregistrement d'une vidéo. Les deux Torontois planifiaient de mettre sur YouTube une vidéo « pyrotechnique » où on les verrait imbiber d'essence à briquet certaines parties de leurs vêtements et les mettre en feu. Ils ont entraîné puis forcé une copine à en faire autant, ce qui lui a causé des blessures. Les vidéos en question ont été utilisées en cour pour apprécier la teneur des événements et l'absence de consentement de la jeune femme.

Questions à vérifier

- *Le participant est-il conscient que ce qu'il écrit et partage, même de façon privée, peut être utilisé à des fins judiciaires ou disciplinaires ?*

3. Comment évaluer ces risques ?

a. La présence d'un moyen de dénoncer le contenu inapproprié

Les sites de partage de contenu vont en général mettre à la disposition des usagers un moyen simple de dénoncer un contenu qui pourrait être considéré comme inapproprié. Par exemple, les sites peuvent joindre à chaque vidéo un lien qui conduit à un formulaire de plainte. Ces liens se reconnaissent habituellement par la présence d'un drapeau et de la mention « *Flag this video* ». Donc, si une personne trouve une vidéo au contenu illégal, il suffit de cliquer sur le lien et de remplir le formulaire pour que la vidéo soit retirée. Certains sites, par contre, limitent la possibilité de faire des plaintes aux membres du site, ce qui réduit le nombre de personnes pouvant le surveiller.

---

80 *R.* c. *Mason*, 2008 BCPC 147 (CanLII).

81 Andrew BLANKSTEIN, « Daredevil tagger gets nearly 4 years in prison », *Los Angeles Times*, 11 septembre 2009.

82 *R.* v. *P. (A.P.)*, 2008 ONCJ 196 (CanLII).

Les sites peuvent également prévoir une procédure de plainte spécifique lorsqu'une personne ou une entreprise veut faire retirer un contenu dont elle détient les droits d'auteur. Cette procédure est généralement calquée sur la procédure de notification d'une infraction au droit d'auteur prévue dans la législation américaine.[83]

> ***Questions à vérifier***
> - *Est-ce qu'il y a une procédure disponible pour faire des plaintes concernant le contenu ? Si oui, est-ce que la procédure est simple et accessible ?*
> - *Faut-il être membre du site pour réguler le contenu qui s'y trouve ?*

b. Le caractère anonyme ou non des participants

Selon le type de site, les publications anonymes peuvent être autorisées ou non. Par contre, la plupart des sites de partage ne permettent pas les soumissions anonymes ni les commentaires anonymes suite au visionnement d'un fichier. Lorsqu'il faut fournir ses coordonnées, comme son adresse de courriel, ou qu'il faut s'enregistrer sur le site pour y participer, les risques de comportements ou de propos inappropriés sont minimisés puisque les participants sont susceptibles d'être identifiés.

> ***Questions à vérifier***
> - *Est-ce que les participants communiquent dans l'anonymat ?*
> - *Est-ce que les participants utilisent des pseudonymes ?*
> - *Est-ce qu'il y a des restrictions quant aux personnes pouvant publier un commentaire ?*

c. Les caractéristiques de l'usager

Les caractéristiques de l'usager, en particulier l'âge et le degré de maturité, influent sur l'ampleur des risques. Dans les sites de partage de contenu par les utilisateurs ce n'est pas le site qui décide ce qu'il publie…mais les utilisateurs eux-mêmes.

> ***Questions à vérifier***
> - *Quel est le public visé par le site de partage de contenu ?*
> - *Est-ce que l'on retrouve du contenu qui pourrait être inapproprié pour le public visé sur le site de partage de contenu ?*

d. La présence de modération

Comme l'ajout de commentaires est possible sur les sites de partage de contenu, les risques de dérapage sont minimisés lorsqu'il y a présence de modération sur le site. La modération peut se faire *a priori*, c'est-à-dire avant que le message soit publié sur

---

83 *United States Code* (17 U.S.C. § 512 (1996)).

Internet, ou encore *a posteriori*, qui signifie que le message sera immédiatement publié, avec la possibilité de le retirer si le contenu s'avère illicite.

S'il n'y a pas de modération, c'est lorsque la personne qui administre le site a connaissance du caractère illicite d'un document qu'elle a l'obligation d'agir et de le retirer[84].

Les visiteurs aussi peuvent avoir un certain contrôle sur les commentaires publiés. Pour éviter que des entreprises ou des personnes utilisent la zone de commentaires comme endroit publicitaire, certains sites permettent aux participants de supprimer des messages en les signalant comme étant du pourriel (*spam*).

Questions à vérifier

- *Est-ce que l'espace réservé au contenu est modéré ? Si oui, de quelle façon ? Cela se fait-il avant ou après la publication d'un commentaire ?*
- *Les visiteurs ont-ils la possibilité de modérer certains commentaires ?*

4. Quelles sont les précautions à prendre ?

a. Informer les participants des risques reliés à l'usage des sites de partage de contenu

Il est important de sensibiliser les usagers aux risques auxquels ils s'exposent en utilisant les sites de partage de contenu, que ce soit pour la préservation de leurs renseignements personnels ou pour la protection du droit d'auteur.

b. Penser aux conséquences possibles avant la mise en ligne de matériel

Il est important de méditer sa décision avant de mettre en ligne du contenu sur un site de partage et réfléchir aux implications possibles lorsqu'on est filmé, surtout si ces images pourraient un jour se retourner contre soi (nudité, ébriété, etc.).

c. S'assurer, avant de publier un fichier, que le site choisi offre un système de modération

La modération est importante pour éviter que des commentaires désobligeants se retrouvent sur un site de partage de contenu. Avant de publier du contenu sur un site, il faut s'assurer que ce dernier offre un service de modération et vérifier si ce service est complet. Les risques de dérapage sont limités si la publication de commentaires est limitée aux seuls membres du site ou si la modération se fait *a priori*.

84 *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 22.

d. Éviter de mettre en ligne des renseignements personnels

Il ne faut pas mettre en ligne des vidéos qui pourraient nuire à ses proches ou à soi-même et vérifier que personne dans son entourage ne le fait. De plus, lors de l'inscription sur un site de partage de contenu, il est préférable de fournir le minimum d'informations personnelles.

e. Éviter de porter atteinte aux droits d'autres personnes

Il faut évidemment s'abstenir de publier tout matériel obscène ou haineux ou constituant une atteinte au droit d'auteur. Il faut obtenir le consentement des personnes identifiables sur les images mises en ligne, surtout si elles sont compromettantes. Il est important de respecter les lois en vigueur de son pays.

De plus, comme de nombreux sites de partage de contenu fonctionnent sur un système de « *flagging* », les usagers ont un rôle très important puisqu'ils peuvent dénoncer les contenus inappropriés aux administrateurs des sites de partage de contenu. On peut ainsi mettre fin à la diffusion d'images ou vidéos illicites.

f. Établir une politique d'utilisation du site de partage de contenu

Quant au site de partage de contenu, il doit établir des règlements quant à l'utilisation de son service. Il peut, entre autres, interdire la publication de contenu à caractère sexuel, raciste, violent, etc. Si les conditions d'utilisation ne sont pas respectées, le site peut se réserver le droit de supprimer le contenu ou de fermer le compte du membre.

g. Mettre sur pied un processus de vérification du contenu

Que ce soit par les utilisateurs ou par les administrateurs du site de partage de contenu, il serait prudent de mettre en place une procédure de vérification du contenu. La procédure de vérification du site par les utilisateurs peut être une bonne alternative. Il s'agit d'inviter les gens à dénoncer un contenu illicite, par une méthode facile offerte par le site. En plus de disposer d'un plus grand nombre de vérificateurs puisque tous les visiteurs peuvent dénoncer un fichier, cette méthode n'engagera pas la responsabilité du site, à moins qu'il ait été averti de l'existence d'un contenu illicite et qu'il ne l'ait pas retiré.

C. Les blogues

La nature du blogue en fait un environnement à la fois de publication et d'hébergement. Certains messages émanent de l'auteur du blogue qui a pris la décision de les diffuser sur le site. D'autres messages peuvent émaner de tiers qui ont répondu à un billet ou qui ont inséré une nouvelle rubrique. Lionel Thoumyre explique que « l'internaute responsable d'un blogue sera, *a priori*, considéré comme un éditeur de service de communication en ligne s'agissant des contenus qu'il publie lui-même volontairement

et comme un organisateur de forums pour les fils de discussion figurant à la suite des articles »[85].

1. Qu'est-ce qu'un blogue ?

Un blogue, appelé également « carnet Web » ou « cybercarnet », est un site Web personnel qui s'apparente à ce qu'on décrit traditionnellement comme étant un journal de bord. La personne qui anime un blogue, soit le blogueur, publie périodiquement sur son site des articles ou billets sur des sujets divers, classés du plus récent au plus ancien.

En général, un blogue sera mis à jour régulièrement par une seule personne qui en aura le contrôle, mais il est possible également que plusieurs auteurs y participent. Les lecteurs et visiteurs du blogue ont généralement la possibilité de publier un commentaire à la fin de chaque billet, de façon anonyme ou non. Il est à la discrétion du blogueur de modérer ou non les opinions publiées pour éviter que des messages illicites se retrouvent sur le site Web.

Les billets qui sont publiés sur les blogues traitent de sujets très variés, tels l'actualité, le sport, le cinéma, les voyages, ou encore les pensées personnelles du blogueur, au même titre qu'un éditorial dans un journal. Le principe est la liberté de parole, sous réserve des propos interdits par la loi, par exemple la propagande haineuse. Il est possible de faire des hyperliens vers d'autres blogues et d'autres sites Internet ou encore de faire des liens à l'intérieur du blogue lui-même, vers des billets plus anciens traitant ou non du même sujet.

Cette façon de créer un site Web se caractérise par sa grande facilité, ce qui explique en partie la popularité des blogues. En effet, aucune connaissance informatique n'est vraiment requise pour créer et mettre à jour un blogue, contrairement à un site Web traditionnel[86]. Le mode de création et de mise à jour très simplifié d'un blogue permet d'économiser beaucoup de temps. Il suffit de s'inscrire sur un site Internet gratuit qui héberge des blogues et de suivre les instructions (voir, par exemple, le site http://www. blogger.com/, qui propose de l'hébergement de blogues gratuitement[87]). Ces sites permettent à tous de créer un blogue personnalisé avec un minimum de connaissances informatiques.

---

85 Lionel THOUMYRE, « La responsabilité pénale et extra-contractuelle des acteurs de l'Internet », Lamy, droit des médias et de la communication, juin 2007, étude 464.

86 En effet, la tenue d'un site Web traditionnel nécessite généralement la connaissance du langage HTML et sa mise en ligne est souvent ardue.

87 *Blogger.com* est la plateforme de blogues le plus populaire au monde (8e site le populaire au monde, toutes catégories confondues, 10e au Canada). Google en est propriétaire. Wordpress.com arrive au second rang (19e site le plus populaire au monde, toutes catégories confondues, 23e au Canada).

On constate également que de plus en plus, les différents types de sites Web se confondent. Par exemple, il est maintenant possible d'intégrer des vidéos puisées sur YouTube à un blogue, ou de bloguer en utilisant un site de réseautage social comme Facebook ou un site de partage de contenus comme YouTube (vidéoblogue).

a. Qui fait quoi ?

i) L'hébergeur

Tout site, forum, blogue ou image accessible sur Internet est, dans les faits, stocké sur un serveur. Dans le cas de blogues, un hébergeur met à la disposition d'usagers, gratuitement ou non, ses serveurs pour stocker les données d'utilisateurs[88]. L'hébergeur fournit l'espace au blogueur, mais il peut aussi être responsable des propos qui y sont tenus lorsqu'il a connaissance de leur caractère illicite. L'hébergeur peut aussi se voir obliger de dévoiler l'identité de blogueurs qui ont des agissements illicites.

ii) Le blogueur

Le blogueur est le créateur d'un blogue. Il peut publier sur son blogue des textes, généralement courts, des photos et des extraits musicaux.

La conception d'un tel site peut se faire grâce à une plateforme d'auto-publication et d'hébergement des blogues ou bien à partir d'un logiciel de publication. La conception du blogue peut aussi se faire indirectement par le blogueur, par l'intermédiaire d'un tiers avec lequel il est lié par contrat (exemple : contrat de travail, de stage, de prestation de service).

iii) Le visiteur

Le visiteur est un acteur important du blogue. En effet, chaque article publié sur un blogue peut être commenté par ceux qui le visitent et devenir le point de départ d'une discussion. C'est l'essence même d'un tel site.

Certains blogues exigent des visiteurs de s'identifier avant de pouvoir laisser un commentaire sur le site alors que d'autres sont ouverts à tous. Cela est à la discrétion du blogueur et permet une identification dans le cas de commentaires illicites.

iv) L'agrégateur

Un agrégateur (de l'anglais *aggregator*) est en fait un logiciel qui permet de suivre plusieurs fils de syndication simultanément.

---

88 « Manuel d'utilisation », Over-blog, en ligne : http://www.over-blog.com/manual/section-glossary_websitehosting.html (site consulté le 19 décembre 2011)

Les fils de syndication sont très utilisés sur les blogues. En fait, chaque nouveau billet publié est transmis, en quasi-temps réel, aux personnes abonnées au fil du carnet qui peuvent le lire directement dans leur agrégateur[89]. L'abonné n'a donc pas besoin de visiter tous les sites pour connaître les mises à jour.

b. Utilisation des blogues

Certaines entreprises ont intégré des blogues dans leurs activités. Il existe deux formes de blogues qui sont entretenus par les entreprises : les blogues internes et les blogues externes.

Les blogues internes servent généralement à favoriser la communication dans l'entreprise. Ils sont accessibles uniquement à partir de l'intranet de l'entreprise. Ils peuvent donc être utilisés à des fins de discussions entre employés, portant sur des problématiques ou des sujets reliés à l'entreprise, ou à la communication entre les différents paliers ou départements de l'entreprise.

Les blogues externes, eux, sont disponibles au grand public de l'Internet. Ils servent alors à communiquer avec les consommateurs ou avec les autres entreprises. Ils peuvent être une vitrine pour annoncer de nouveaux produits et des concours, expliquer des politiques et réagir aux foudres de l'opinion publique[90]. Les blogues externes peuvent être ouverts aux commentaires des utilisateurs. Dans ce cas, ils peuvent servir d'outil de rétroaction par les consommateurs.

Il existe aussi des blogues qui sont maintenus par des employés d'entreprises ou d'organismes publics où ceux-ci diffusent, entre autres, des articles, des commentaires ou des découvertes récentes (exemple : blogues de professeurs universitaires).

2. Quels sont les risques associés aux blogues ?

Cette section aborde les enjeux juridiques liés au fait de diffuser des contenus, généralement écrits, de façon **personnelle, publique** et **informelle,** sur des sites permettant des échanges entre les internautes, notamment par la possibilité de faire des **commentaires**. Notons que les forums de discussions et babillards entrent aussi dans cette catégorie puisqu'ils partagent des enjeux similaires.

a. Les atteintes à la réputation, la propagande haineuse et les menaces

Un blogue peut être un moyen facilitant la diffusion d'informations susceptibles de constituer des atteintes à la réputation, de la propagande haineuse, ou des menaces. En

---

89 WIKIPÉDIA, « Agrégateur », en ligne : http://fr.wikipedia.org/wiki/Agr%C3%A9gateur (site consulté le 19 décembre 2011)

90 WIKIPÉDIA, "Corporate blog", en ligne: http://en.wikipedia.org/wiki/Corporate_blog (site consulté le 19 déecembre 2011)

effet, aucune connaissance technique n’est vraiment requise pour y publier des textes et il s’agit là d’un média accessible à un grand nombre de personnes.

Dans ces conditions, une personne mal intentionnée peut facilement promouvoir, au moyen de son blogue, des idées qui peuvent constituer une atteinte à la réputation d’une personne, comme des insultes ou des propos humiliants. Par exemple, dire qu’un politicien souffre de détérioration mentale et qu’il est paranoïaque pourrait être considéré comme une atteinte à la réputation.

Il est facile aussi de diffuser des propos racistes et homophobes, constituant de la propagande haineuse, qui est d’ailleurs sanctionnée aux articles 318 et 319 du *Code criminel*. Une personne peut aussi menacer quelqu’un sur son blogue en diffusant, par exemple, des menaces de causer la mort. La diffusion de menaces est également un crime prévu au *Code criminel*.

Certaines personnes utilisent un blogue au nom de quelqu'un d'autre pour lui nuire, en mettant, par exemple, des photos compromettantes ou en lui attribuant des propos gênants.

Un employé doit éviter de diffuser dans un blogue des détails sur sa vie professionnelle ou son employeur, en particulier des données confidentielles (secrets commerciaux) ou des médisances sur ses collègues, ses supérieurs ou ses compétiteurs.

Questions à vérifier

- *A-t-on sensibilisé l’employé au fait que son comportement doit être conforme aux politiques de l’entreprise/organisme, et ce, même en utilisant le matériel à la maison ?*
- *L'entreprise a-t-elle fait connaître à l'employé les informations considérées privilégiées (par exemple, certaines informations financières cotées en bourse) ?*
- *Est-ce que les faits présentés sur le blogue sont vérifiés et vérifiables ?*
- *Est-ce qu’il y a présence de modération sur le site ?*
- *Quel est le sujet traité sur le blogue ? Est-ce un sujet qu'il est permis ou interdit d'aborder selon la politique d'utilisation de l'entreprise ?*
- *Sommes-nous appelés à révéler des renseignements personnels, confidentiels ou privilégiés sur notre blogue ?*

b. La présence de contenu inapproprié

Puisque certains blogues vont couvrir des dizaines de sujets différents et non un seul en particulier, il devient difficile d’éviter complètement l’exposition à un contenu offensant. Il est possible, par exemple, de naviguer sur un blogue traitant de voyage et se retrouver sur un récit à caractère sexuel. Il y a, par contre, des sites d’hébergement de blogues qui sont consacrés uniquement à la publication de contenu à caractère sexuel, il devient donc plus facile d’éviter ces sites, si telle est notre intention.

La pornographie ne convient généralement pas à un certain auditoire comme les enfants, mais elle n'est pas nécessairement illicite. Elle peut constituer un geste équivalent à du harcèlement dans certaines circonstances. Nous pouvons retrouver, sur un blogue, du contenu illégal qui peut prendre la forme de matériel obscène, de bestialité ou encore de pornographie juvénile.

Questions à vérifier
- *Quel est le sujet du blogue en question ? Est-ce que le sujet convient au public visé ?*

c. La divulgation de renseignements personnels et confidentiels

Un des plus grands risques des blogues est la facilité avec laquelle il est possible d'y dévoiler des renseignements personnels nous concernant ou concernant les autres. En effet, plusieurs personnes utilisent les blogues pour raconter des anecdotes ou encore parler de leur vie personnelle comme ils le feraient dans un journal intime. Il devient risqué, à ce moment, que des informations, comme une adresse de courrier électronique ou encore un numéro de téléphone, soient dévoilées, que ce soit volontairement ou non. La divulgation de coordonnées personnelles doit être faite avec précaution.

De même, relater sa vie professionnelle sur un blogue peut amener à révéler, par mégarde, des informations confidentielles, des listes de clients ou des secrets commerciaux.

Les blogues deviennent pour certains un espace où raconter des histoires intimes, ce qui peut générer des atteintes à la vie privée. Souvent, sous le couvert de l'anonymat, les internautes se croient permis de raconter des histoires intimes, parfois en nommant les personnes impliquées ou en donnant des détails qui peuvent les rendre identifiables. Par exemple, une dame qui tient un blogue où elle discute de sa vie sociale ainsi que des relations sexuelles qu'elle entretient avec des hommes pourrait porter atteinte à la vie privée des personnes avec qui elle a des relations. Si elle n'a pas leur consentement pour publier ces informations intimes, elle s'expose à des poursuites judiciaires.

Questions à vérifier
- *L'entreprise a-t-elle fait connaître à l'employé les informations considérées privilégiées ou confidentielles (par exemple, certaines informations financières cotées en bourse) ?*
- *L'entreprise a-t-elle mis en place des mesures de protection qui amèneraient les employés à conclure que ces informations sont confidentielles ?*
- *Le blogueur est-il amené à dévoiler des renseignements personnels ou confidentiels sur lui-même ou sur une autre personne (et l'entreprise/organisme public…) ?*
- *Le blogueur est-il au courant des risques inhérents à l'utilisation de cet outil ?*

d. La responsabilité pour les informations diffusées

i) Responsabilité du blogueur pour les textes qu'il publie

Un blogueur est le premier responsable de l'information qu'il publie lui-même sur son blogue. Il a le contrôle sur ce qui est écrit dans les textes qu'il publie et il peut décider qui aura accès à la diffusion. Dans cette situation, il peut être qualifié d'éditeur, ce qui fait en sorte que les exonérations de responsabilités prévues dans la *Loi concernant le cadre juridique des technologies de l'information* ne s'appliqueront pas à lui.

ii) Responsabilité du blogueur à l'égard des commentaires émanant de tiers

À l'égard des commentaires publiés par des tiers sur le blogue, des distinctions doivent être faites. Un blogueur qui exerce une modération attentive de tous les commentaires pourrait être tenu responsable si des propos illicites se retrouvent publiés. Dans une pareille hypothèse, l'on peut en déduire qu'il a approuvé les commentaires. Si le blogueur n'exerce pas de modération, ce n'est que lorsqu'il aura été est informé de la présence sur son blogue d'un document illicite qu'il aura l'obligation d'agir et de le retirer si nécessaire[91]

Question à vérifier
• *Est-ce que le blogueur a accès à un système de modération des commentaires sur son blogue ? Est-ce que cette fonction est activée ?*
• *Le blogueur agit-il pour le compte de l'entreprise/organisme ?*

e. La diffusion des images des personnes

Lorsque le blogue présente des photographies, il y a un risque d'atteinte au droit à l'image de la personne. Les blogues personnels, par exemple, contiennent parfois des photographies des amis du blogueur ou d'événements auxquels il a participé avec d'autres personnes. L'utilisation de ces images, lorsque les personnes photographiées sont identifiables, risque de brimer leur droit à l'image. Une photo d'une personne ne peut donc pas être utilisée si elle n'a pas donné son consentement. L'insertion, dans son blogue, d'un lien qui mène vers la photographie de quelqu'un pourrait même être une source de litige possible.

Question à vérifier
Est-ce qu'il y a des personnes identifiables à travers le contenu ?
Est-ce que le blogueur a l'autorisation de publier la photo de la personne ?

---

91 Art. 22, *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1; Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique», dans Vincent GAUTRAIS, *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 607-649.

f. Les atteintes au droit d'auteur et aux marques de commerce

Le blogueur peut parfois emprunter des images ou des œuvres provenant d'autres sites Internet ou d'ailleurs. Des questions de droit d'auteur et de droit des marques de commerce peuvent alors se poser. En effet, pour publier une œuvre à l'égard de laquelle on ne détient pas les droits, il faut obtenir la permission de celui qui détient ces droits selon la *Loi sur le droit d'auteur*. Cette permission peut parfois s'avérer difficile à obtenir, en particulier pour les images puisqu'elles peuvent être reproduites d'un site à l'autre. On peut ainsi perdre la trace de la provenance initiale de l'œuvre.

Un blogueur américain a été condamné à un an de probation pour avoir mis en ligne neuf chansons tirées de l'album *Chinese Democracy* de Guns N' Roses. La Cour fédérale a aussi obligé le blogueur à enregistrer un message anti-piratage pour la *Recording Industry Association of America*[92]. En France, Google a été condamné à verser des dommages à Benetton pour les comportements illicites d'une blogueuse qui reproduisait sur son blogue, hébergé par Google, la marque Benetton et des photos issues du catalogue[93].

Lorsqu'on établit des liens hypertextes, il faut également s'assurer de respecter le droit d'auteur. Des techniques consistant à reproduire le site à l'intérieur du blogue (*framing*) ou encore à copier la banque de liens hypertextes d'un autre site peuvent s'avérer risquées.

Questions à vérifier

- *Est-ce que les articles du blogue contiennent des œuvres ou parties d'œuvres qui sont protégées par la* Loi sur le droit d'auteur *?*
- *Est-ce que le blogueur détient les autorisations nécessaires pour publier tout ce qui se trouve sur son blogue ?*
- *Si l'entreprise se qualifie d'hébergeur, a-t-elle une procédure afin de s'assurer d'agir promptement pour rendre inaccessible le matériel illicite ?*

g. La consultation décontextualisée

Dans certains cas, tenir un blogue permet de montrer son savoir-faire à des employeurs potentiels ou tient lieu d'autopromotion. Or, parfois, des blogueurs relatent des

92 Anthony MCCARTNEY, « Un blogueur écope d'un an de probation pour avoir violé le droit d'auteur », Associated Press, Technaute.ca, 14 juillet 2009, en ligne : http://technaute.cyberpresse.ca/nouvelles/internet/200907/14/01-884129-un-blogueur-ecope-dun-an-de-probation-pour-avoir-viole-le-droit-dauteur.php

93 *Google Inc. / Benetton*, Bencom, Cour d'appel de Paris 14e chambre, section A, 12 décembre 2007. Après que Benetton ait signalé les contenus manifestement illicites, l'hébergeur Google n'a pas agi promptement pour rendre inaccessible le blogue litigieux et s'est a donc vu sa responsabilité engendrée pour les dommages causés.

histoires sur leur vie professionnelle, leur employeur ou leurs collègues de travail ce qui peut conduire à des réprimandes et même à un congédiement.

Au Québec (comme dans plusieurs autres endroits), l'employeur mécontent du blogue tenu par un employé peut congédier celui-ci, et ce, sans préavis, si ses propos constituent une faute grave ou si l'employé a manqué à son devoir de loyauté (par exemple, en divulguant un secret professionnel ou en tenant des propos insultants sur la compagnie). Contrairement aux sites de réseautage social, le caractère généralement public des blogues empêche toute attente raisonnable de respect de la vie privée par l'employé face à son employeur ou son potentiel employeur, et ce, même s'il agit anonymement.

L'américaine Heather Armstrong a été congédiée en 2002 pour des propos qu'elle tenait sur son blogue www.dooce.com, notamment un billet où elle décrivait de façon humoristique les raisons pour lesquelles elle ne devrait pas pouvoir travailler de son domicile, par exemple « *too many cushiony horizontal surfaces prime for nappage*[94] ». Bien qu'elle n'y nommait ni son employeur ni aucun de ses collègues, son site a été découvert et elle en a subi les conséquences. Et « *to be dooced* » est devenue l'expression consacrée chez les blogueurs américains pour exprimer le fait de se faire congédier pour des propos publiés sur son blogue.

Le professeur Erik Ringmar, de la *London School of Economics* (LSE) a été réprimandé pour avoir publié sur son blogue les propos de la conférence qu'il avait donnée pour faire la promotion de son établissement auprès de potentiels étudiants. À un moment de son discours, il disait qu'en raison de l'importance accordée à la recherche, les professeurs étaient peu disponibles et qu'essentiellement, c'était les étudiants au doctorat qui dispensaient la formation. Le directeur de son département ainsi que le directeur général de LSE l'ont sommé de retirer le billet « diffamatoire » de son blogue, ce qu'il a fait, tout en déplorant l'accroc à la libre expression[95].

D'autre part, selon les milieux professionnels, tenir un blogue peut s'avérer un moyen d'auto-promotion pour se faire connaître des employeurs et pour démontrer ses compétences, que ce soit pour un informaticien ou un artiste.

h. L'utilisation des blogues à des fins judiciaires ou disciplinaires

Les blogues personnels ou d'organisations se révèlent souvent de plus en plus élaborés et faciles d'accès. De plus, il est désormais beaucoup plus facile de les conserver en ligne. Tout propos exprimé sur un blogue et accessible au public peut éventuellement servir en preuve dans le cadre de procédures judiciaires. Ainsi, des photos ou vidéos mis

94 http://www.dooce.com/archives/daily/06_27_2001.html

95 « Lecturer's Blog Sparks Free Speech Row », Donald MacLeod, *The Guardian*, 3 mai 2006, http://www.guardian.co.uk/education/2006/may/03/highereducation.economics

en ligne volontairement ou non peuvent se révéler problématiques pour les personnes visées s'ils présentent des activités pouvant constituer des infractions. Dans d'autres situations, des informations, en elles-mêmes anodines, pourraient être utilisées en contexte judiciaire afin de miner la crédibilité d'une personne.

> ***Question à vérifier***
> - *L'utilisateur est-il conscient de l'usage judiciaire ou disciplinaire qui peut être faite des informations publiées, et ce même s'il agit anonymement ou s'il les retire ?*
> - *Les écrits, les photos et les vidéos publiés pourraient-ils éventuellement nuire à la personne visée ou à ses proches ?*

3. Comment évaluer ces risques ?

La portée des risques que représentent les blogues sera plus ou moins importante selon ces facteurs : la présence de modération, l'anonymat des participants, le sujet traité et la présence de sons, d'images ou encore de vidéos.

a. La présence de modération

Lorsqu'il y a présence de modération sur le blogue, les risques sont minimisés. La modération peut se faire *a priori*, c'est-à-dire avant que le message soit publié sur Internet, ou encore *a posteriori*, qui signifie que le message sera immédiatement publié, avec la possibilité de le retirer si le contenu est jugé illicite.

S'il n'y a pas de modération sur le blogue, c'est lorsqu'il a connaissance du caractère illicite d'un propos publié que le blogueur a l'obligation d'agir et de le retirer, si cela s'avère nécessaire[96].

> ***Question***
> - *Est-ce que le blogue est modéré ? Si oui, de quelle façon ? Cela se fait-il avant ou après la publication d'un commentaire ?*

b. Le caractère anonyme ou non des participants

L'anonymat des personnes qui tiennent un blogue ou qui commentent les billets des autres est aussi un facteur qui accentue les risques. Généralement, les hébergeurs recueillent certains renseignements personnels, comme l'adresse IP du blogueur et de ceux qui publient des commentaires. Ils peuvent proposer également au blogueur, au sein du service de modération, d'interdire les commentaires anonymes. On peut, par exemple, restreindre la possibilité de commenter les billets aux seuls membres du site Internet.

---

[96] Art. 22, *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1.

Par contre, lorsqu'il n'y a aucune mesure de contrôle, la publication de billets ou de commentaires au contenu illicite est facilitée puisque l'auteur sait qu'il est difficile de le retracer. Pourtant, il existe des moyens légaux et techniques pour retracer les auteurs anonymes et plusieurs ont été menacés devant les tribunaux de voir leur identité dévoilée et ainsi être appelés à répondre des informations illicites qu'ils ont mis en ligne.

Questions à vérifier

- *Est-ce que les participants communiquent dans l'anonymat ?*
- *Est-ce que les participants utilisent des pseudonymes ?*
- *Y a-t-il - des restrictions quant aux personnes pouvant publier un commentaire ?*

c. Le sujet traité

Le traitement de certains sujets est plus risqué que d'autres. Il n'y a pas toujours un sujet précis qui est traité dans un blogue. Bien souvent, c'est un mélange de plusieurs sujets, qui peuvent varier entre l'actualité et la vie personnelle du blogueur, au gré de ses intérêts. Une personne peut donc avoir accès à un billet ne convenant pas à son âge, par simple inadvertance. Par contre, lorsqu'un sujet en particulier est développé sur un blogue, par exemple un sujet « chaud », il convient de faire preuve de prudence et de s'assurer que le contenu du site est convenable pour le public visé.

Questions à vérifier

- *Est-ce que le blogue traite de sujets qui sont définis clairement ? Y a-t-il - plusieurs sujets ou est-ce un sujet en particulier ?*
- *Est-ce que le sujet traité convient à l'âge des participants ?*

d. La présence de sons, d'images ou de vidéos

Lorsqu'un blogue fait appel à des sons, images ou vidéos, peuvent s'ajouter des risques d'atteinte aux droits d'auteur ou aux droits des marques, si les éléments utilisés n'appartiennent pas au blogueur ou s'ils ne sont pas autorisés.

Les blogues peuvent aussi contenir la photographie du blogueur, ou de toute autre personne, comme les participants. Des problèmes de divulgation de renseignements personnels peuvent alors se poser ainsi que de droit à l'image.

Questions à vérifier

- *Y a-t-il présence de sons, d'images ou de vidéos sur le blogue ? Si oui, est-ce que le blogueur détient les autorisations nécessaires pour les utiliser ?*
- *Est-ce que le blogue présente l'image de participants ?*

4. Quelles sont les précautions à prendre ?

a. Établir une politique d'utilisation du site d'hébergement de blogues

Le site d'hébergement de blogues doit établir des règlements quant à l'utilisation de son service. Il pourrait, entre autres, interdire les blogues à caractère sexuel ainsi que ceux qui propagent un message de racisme ou de violence. Si les conditions d'utilisation ne sont pas respectées, le site peut se réserver le droit de fermer le blogue.

b. S'assurer, en créant un blogue, que l'hébergeur choisi offre un système de modération

La modération est importante pour éviter que des commentaires désobligeants se retrouvent sur un blogue. En choisissant un hébergeur de blogue, il est prudent de s'assurer qu'il fournit un service de modération complet, par exemple en limitant la publication de commentaires aux seuls membres du site ou en offrant la modération *a priori*. Au minimum, il faut s'assurer que les tiers qui estiment qu'un document sur le blogue est illicite puissent le notifier au responsable du blogue afin que celui-ci retire le contenu lorsque son caractère illicite est confirmé.

c. Énoncer les règles de conduite des participants ou Nétiquette

Comme il est difficile de délimiter ce qui constitue un comportement interdit de ce qui relève de l'exercice de sa liberté d'expression, des règles de conduite doivent être énoncées pour informer les participants des propos et gestes qui sont considérés comme inacceptables sur le site. Par exemple, un blogueur peut, dans ses règles de conduite ou sa Nétiquette, avertir les participants qu'il est interdit de publier des commentaires qui portent atteinte à la réputation de personnes identifiables.

Une politique d'utilisation d'un blogue[97] doit indiquer aux tiers qu'ils sont responsables des propos qu'ils diffusent, et se réserver le droit de retirer des commentaires qui seraient contraires à la loi. La modération *a priori* des commentaires implique un choix éditorial qui pourrait rendre le blogueur responsable des contenus publiés par les tiers.

Il faut également indiquer un moyen de rejoindre l'auteur du blogue, et encourager les internautes à dénoncer les contenus contraires à la loi, que ce soit de la diffamation ou de l'incitation à la haine.

Plus précisément, dans le cas d'une entreprise, la politique d'utilisation d'Internet peut prévoir une section sur les blogues (permission ou interdiction pour les employés de nommer l'employeur ou d'aborder certains sujets; conséquences en cas de violation de

---

97 Voir par exemple la politique du réseau Canoë, disponible au http://fr.canoe.ca/reference/politique.html

la politique). Cela est notamment souhaitable si l'entreprise entretient un blogue corporatif ou si elle encourage les employés à mettre sur pied leur propre blogue.

Même si le blogue est anonyme, l'employé devrait s'informer de la politique de l'employeur à l'égard des blogues, car il pourrait éventuellement être identifié. Ainsi, l'employé devrait éviter de donner des détails sur sa vie professionnelle ou son employeur, et plus particulièrement des données confidentielles (exemple : secret commercial, renseignements personnels) ou des médisances sur ses collègues ou supérieurs.

De plus, il importe pour l'employé de connaître (et pour l'employeur de faire connaître) les informations considérées privilégiées (par exemple, certaines informations financières d'entreprises cotées en Bourse).

D'autre part, le professionnel qui écrit un blogue doit garder en tête son code de déontologie et, notamment, le respect du secret professionnel (avocat, psychologue, etc.)

Tout comme pour les sites de partage de contenus, l'employé devrait s'assurer de ne pas mettre en ligne des photos ou des histoires compromettantes sur son blogue. Par exemple, il pourrait être nuisible de parler de ses aventures sexuelles ou de ses expériences de consommation de drogues (ou de les montrer en photos !).

L'employé devrait également s'abstenir d'alimenter son blogue à partir de son lieu de travail, ce qui pourrait révéler son identité et éventuellement entraîner des sanctions pour vol de temps ou usage inapproprié du matériel de l'employeur. Le contrat de travail peut contenir des clauses relatives aux blogues, passant de l'interdiction complète à la cession à l'employeur de tous ses droits d'auteur sur les contenus publiés en ligne.

Les employeurs utilisent de plus en plus des systèmes automatisés pour vérifier l'utilisation du nom de l'entreprise sur le Web et les possibles infractions à leur propriété intellectuelle

d. Informer les participants des risques liés à l'usage des blogues

Il est important de sensibiliser les participants aux risques auxquels ils s'exposent en utilisant les blogues, que ce soit pour la protection de leurs renseignements personnels ou pour la protection du droit d'auteur.

e. Bonnes pratiques pour minimiser les risques d'atteintes aux droits

Il faut éviter de mettre en ligne du contenu (texte, photo, dessin, vidéo, etc.) pour lequel on n'a pas les droits ou la permission du détenteur de droits.

Si l'objet (image ou vidéo) résulte d'un travail en équipe, il faut s'assurer que les co-blogueurs ne contreviennent pas au droit d'auteur, car tous pourraient être tenus solidairement responsables. De plus, lors d'un partage de blogue (par exemple, si trois personnes rédigent un blogue), la personne qui écrit un texte conserve le droit d'auteur sur ce texte, mais le site entier est une œuvre collective (ensemble des billets et des commentaires, structure et apparence du blogue, etc.). Cela signifie que si un co-blogueur décide de quitter le blogue, il peut exiger le retrait de tous ses billets et, dans certaines circonstances, empêcher la continuation du blogue tel qu'il se présentait jusqu'alors[98]. Il peut être intéressant de conclure une convention entre les blogueurs ou, si le blogue est à but lucratif, de former une compagnie.

Si les billets diffusés sur le blogue ont été réalisés dans le cadre d'un emploi, l'employeur est le premier titulaire du droit d'auteur sur ceux-ci. Mais, à leur égard, l'employé conserve à leur égard le droit moral, ce qui inclut le droit à se voir reconnaître la paternité de son œuvre.

Souvent, l'objectif d'un blogue est d'échanger des informations et contenus avec les autres. Sur son blogue, le blogueur devrait indiquer clairement aux internautes son point de vue sur la question, par exemple, si l'internaute doit demander une permission avant de reprendre ses propos.

Il faut distinguer ce qui relève de la vie privée de ce qui relève de la sphère publique. Curieusement, beaucoup de blogues constituent des journaux intimes publics. Il faut alors utiliser son jugement et veiller à protéger l'intimité des personnes impliquées dans les histoires personnelles racontées[99].

D. Le micro-blogue (Twitter)

1. Qu'est-ce qu'un micro-blogue (Twitter) ?

À l'instar d'un blogue, Twitter permet de publier des messages sur une page qui nous est attitrée. Contrairement au blogue traditionnel, le nombre de caractère est limité à 140 par message. Pour cette raison, on catégorise Twitter comme site de *micro-blogging*.

Twitter permet ensuite de s'abonner à d'autres utilisateurs, ce qui permet de les *suivre*. Ainsi, lorsque l'utilisateur ouvre sa page d'accueil, il y retrouve un fil de nouvelles avec tous les messages récents de ses abonnements.

---

98 Eric GOLDMAN, « Co-blogging law », 84 Washington University Law Review 1169.

99 Voir par analogie, *Aubry c. Éditions Vice-Versa inc.*, [1998] 1 R.C.S. 591.

Il convient de signaler que tous les *tweets*, c'est-à-dire messages de moins de 140 caractères, sont *a priori* publics. Nul besoin d'être membre pour lire des messages sur Twitter. L'adhésion au service est gratuite et permet simplement de suivre et d'être suivi par d'autres utilisateurs.

Certaines fonctions rendent l'utilisation de Twitter plus efficace. Il est possible de *Retweeter* un *tweet* que nous recevons sur notre page d'accueil afin d'en faire part à ceux qui nous suivent. On peut répondre aux messages qui apparaissent sur notre page d'accueil. Un utilisateur peut aussi envoyer un message sur la page de profil d'un autre en commençant son message par le symbole @ suivi du nom de l'utilisateur.

Une des fonctions du micro-blogue Twitter est le *hashtag*. Un *hashtag* est un mot-clé précédé du symbole dièse (#). Il sert à répertorier tous les commentaires traitant d'un sujet. Ainsi, un utilisateur pourra utiliser le moteur de recherche afin de trouver un *hashtag* portant sur un sujet qui l'intéresse. En cliquant sur ce *hashtag*, qui prend la forme d'un lien hypertexte, il se retrouvera sur une page qui répertorie, du plus récent au plus ancien, tous les commentaires publiés en lien avec ce sujet.

Le contenu des publications sur Twitter diffère de celui des blogues ou autres outils du Web 2.0. Comme les messages se limitent à 140 caractères, il est d'usage de mettre des hyperliens, afin de rediriger ses lecteurs sur d'autres sites.

Enfin, Twitter permet aussi la création de listes d'abonnements. Les listes d'abonnements peuvent être publiques ou privées. Lorsqu'elles sont publiques, elles peuvent être partagées. Par exemple, un utilisateur peut créer une liste *Université* et ajouter tous les professeurs qu'il connaît qui ont un compte Twitter.

a. Qui fait quoi ?

i) Les usagers

Les particuliers utilisent généralement Twitter pour échanger, partager ou commenter sur toutes sortes de sujet, y compris la vie quotidienne. Les utilisateurs peuvent aussi personnaliser leur page de profil au moyen de photos, de fonds d'écran ou du choix de la couleur de la police.

Les usagers sont généralement des personnes. Il arrive de plus en plus que les entreprises s'abonnent à Twitter pour soutenir des campagnes promotionnelles de type viral ou pour obtenir la rétroaction du public sur certains produits ou services. Les entreprises peuvent aussi payer pour des *Tweets* publicitaires qui seront diffusés sur les pages d'accueil de certains abonnés.

Certaines personnes célèbres bénéficient d'un symbole indiquant que leur compte a été validé. Le compte validé indique que c'est le compte Twitter officiel de la personne. Bien que ce procédé ne soit encore réservé qu'à des célébrités, il peut aider à prévenir le hameçonnage.

Tous les utilisateurs sont soumis à la *Politique d'utilisation de* Twitter, qui comprend un code de conduite ainsi qu'une politique de confidentialité. Contrairement à la plupart des sites où une adhésion est requise, Twitter ne prévoit pas d'âge minimum[100].

ii) Les visiteurs

Les visiteurs sont tous ceux qui visitent ou consultent Twitter sans y participer en tant que membre. Les visiteurs ont accès aux *Tweets* de tous les membres, à l'exception des profils privés. Ils ont aussi la possibilité d'effectuer des recherches. De plus, chaque compte Twitter est muni d'un fil de syndication de données (RSS). Il est donc possible pour un visiteur de suivre les *Tweets* d'un membre sans s'abonner à Twitter.

Les visiteurs peuvent aussi trouver le profil d'un membre de Twitter par un moteur de recherche. À l'instar de la plupart des blogues, chaque compte Twitter est accessible via une adresse URL. À la différence du blogue ordinaire, les visiteurs sur Twitter occupent une moins grande place que les abonnés.

iii) Les abonnés

Les abonnés regroupent tous les usagers membres de Twitter qui suivent un usager précis. Lorsque ce dernier publie un *Tweet*, tous ses abonnés voient le message sur leur page d'accueil. Les abonnés peuvent aussi *Retweeter*. Cette fonction est très importante dans ce réseau. Twitter n'affiche pas le nombre de visites qu'une page a reçues, mais indique le nombre de fois qu'un message a été relayé par *retweet*.

iv) Les développeurs

Les développeurs sont ceux qui créent la plateforme de Twitter. Ils déterminent aussi le contenu de la Politique d'utilisation. Ils se réservent le droit d'intervenir lorsqu'une infraction aux conditions d'utilisation est signalée[101].

b. Utilisation du micro-blogue (Twitter)

Comme c'est le cas pour les blogues, les entreprises, leurs employés et leurs clients peuvent trouver une utilité à se créer un compte Twitter.

Les organismes peuvent l'utiliser d'une façon semblable aux blogues, c'est-à-dire surtout pour tenir le public, les clients informés de l'actualité de l'entreprise ou de l'organisme. Toutefois, Twitter permet une plus grande interaction, puisque n'importe quel usager peut envoyer un message. Twitter permet aussi à l'entreprise d'augmenter

---

100 Voir: Formulaire d'adhésion à Twitter. Conditions d'utilisation de Twitter, disponible en ligne : http://twitter.com/tos.

101 « Twitter : Conditions d'utilisation », *Twitter*, http://en.twitter.com/tos, s. Restriction sur le contenu et l'utilisation des services.

sa crédibilité en partageant son expertise, en proposant des bons de réduction (etc.) pour les « followers », et bénéficier de la rétroaction des consommateurs.

Pour les employés, Twitter peut avoir des usages multiples. Un superviseur peut s'ouvrir un compte et y diffuser des informations à l'intention de ses collègues (liens vers des sources documentaires, précisions sur les travaux à effectuer, activités à venir, etc.). Les employés, sans avoir besoin de s'inscrire sur Twitter, pourront aller chercher les informations en question. Cependant, pour qu'une telle utilisation soit possible, il faut que les messages soient publics, donc accessibles à tous.

Une entreprise pourrait utiliser Twitter pour s'adresser aux consommateurs en se « comparant » à ses compétiteurs. Cependant, il faudra s'assurer que les informations sont vérifiées et véridiques et qu'elles ne sont pas dévoilées dans le seul but de nuire.

Enfin, Twitter est de plus en plus pris au sérieux comme outil de consultation de l'actualité. Twitter perce souvent les nouvelles, et ce, avant les grands médias. À cet effet, le BBC College of Journalism rapporte que Twitter a joué un rôle crucial dans la couverture du séisme à Haïti en 2009. Par la suite, Twitter a été utilisé pour coordonner certaines opérations d'aide aux sinistrés. Il est envisageable que Twitter puisse être utilisé par les institutions scolaires dans leurs mesures d'urgence.[102] Il demeure primordial de comprendre les risques reliés à son utilisation.

2. Quels sont les risques associés au micro-blogue (Twitter) ?

a. La diffusion de renseignements personnels et les atteintes à la vie privée

Twitter invite l'usager à « converser »; la plupart des usagers partagent sur des sujets d'actualité, mais surtout conversent sur eux-mêmes, leur vie familiale, des gens qu'ils ont rencontrés, les endroits qu'ils fréquentent, etc.

Les risques sont similaires à ceux du blogue standard de révéler des informations personnelles sur soi-même ou sur autrui. Comme Twitter permet d'afficher tous les *tweets* d'un usager, il est envisageable d'identifier une personne en cumulant différents indices.

Comme la persistance des *tweets* sur Twitter est encore inconnue, les informations divulguées peuvent demeurer accessibles longtemps après leur publication.

---

102 Matthew ELTRINGHAM, « Has Twitter grown up? », *BBC College of Journalism Blog*, 28 mai 2010, http://www.bbc.co.uk/journalism/blog/2010/05/has-twitter-grown-up.shtml, (site consulté le 19 décembre 2011).

Questions à vérifier

- *Quels renseignements personnels sont divulgués ? Nom complet ? Lieux de fréquentation ? Adresse ? Adresse courriel ?*
- *L'usager fournit-il des renseignements sur d'autres personnes ?*
- *Est-ce que la personne a consenti à ce qu'on donne des informations sur elle ?*
- *Est-ce que la personne est aussi abonnée à Twitter ?*
- *Est-ce que l'usager laisse suffisamment d'indices pour deviner qui est la personne visée (Surnom, lieu de travail, habillement, description physique)?*

b. Les atteintes à la réputation, les propos haineux ou autrement inappropriés

Comme pour le blogue, les risques de diffusion de propos haineux, menaçants, propagandistes ou diffamatoires sont présents sur Twitter. Ces risques sont néanmoins accentués par le caractère décontextualisé qu'impose le maximum de 140 caractères. Une mauvaise blague peut rapidement être interprétée comme une menace.

Le risque est accentué par la fonction *Retweet*. Il est possible en tout temps d'effacer un *Tweet* que l'on a publié. Toutefois, lorsque le message a été republié, via *retweet*, par un autre usager, il n'est plus possible de le supprimer. Il est donc facile de perdre le contrôle sur un message.

De plus, l'utilisateur ne se doute pas nécessairement qu'en 140 caractères, un message peut être lourd d'impacts. Par exemple, une dame aux États-Unis a été poursuivie pour 50 000 $ pour avoir *tweeté* que son appartement était maintenu dans des conditions insalubres par la compagnie de gestion de l'immeuble[103]. La poursuite a cependant été rejetée car le tribunal n'a pas jugé le propos diffamatoire. Mais le droit québécois est beaucoup plus protecteur de la réputation que le droit américain et les risques de poursuites pour des critiques adressées à une entreprise sont plus élevés.

Twitter présente aussi un risque particulier en ce qui concerne les propos haineux. Les usagers qui veulent avoir beaucoup d'abonnés, et qui ne sont pas des célébrités hors Twitter, vont souvent capitaliser sur un sujet particulier qu'ils traiteront à fond. Un usager peut trouver là une tribune pour des blagues à caractère raciste, sexiste ou méprisant à l'endroit de la religion, des handicapés, etc.

Questions à vérifier

- *L'employé est-il informé que son comportement en ligne doit être conforme aux politiques de l'entreprise/organisme et ce, même en utilisant le matériel à domicile?*
- *L'usager identifie-t-il un groupe déterminé dans ses micromessages ?*
- *L'usager nomme-t-il les personnes visées par ses commentaires ?*

---

103 TECHNAUTE, *Cyberpresse*, « Une poursuite de 50 000 $ pour un “ tweet ” diffamatoire », 31 juillet 2009, disponible au : http://technaute.cyberpresse.ca/nouvelles/internet/200907/29/01-888214-une-poursuite-de-50-000-pour-un-tweet-diffamatoire.php (site consulté le 3 juin 2010). Voir aussi : http://en.wikipedia.org/wiki/Horizon_Group_v._Bonnen.

- *L'usager critique-t-il une pratique ou s'adonne-t-il plutôt à des attaques personnelles ?*
- *L'usager encourage-t-il à la haine ou le mépris d'un individu ou d'un groupe identifiable ?*

c. La redirection vers des sites à contenu inapproprié

Ce risque est causé une fois de plus du maximum de 140 caractères. Comme les liens vers les adresses URL des sites Web sont parfois longs, il est possible de les raccourcir. Le site le plus utilisé pour raccourcir les URL est sans doute http://bit.ly. Grâce à ce service, une adresse URL vers un article de journal, qui se lirait comme suit : http://news.bbc.co.uk/2/hi/business/10145993.stm devient http://bit.ly/cnIj9E.

Bien que cela semble très avantageux à première vue, on se rend vite compte que l'on perd le nom de domaine du site auquel on réfère. Outre la confiance en l'usager qui publie le lien, le nom de domaine est la seule référence que l'on a pour juger *a priori* de la qualité du lien. Il est risqué, dès que le lien est publié par un inconnu, d'être redirigé vers des tentatives d'hameçonnage, du contenu offensant, sexuellement explicite, violent ou autrement inapproprié. Heureusement, il existe de plus en plus de méthodes pour visualiser le lien en entier avant de cliquer.

Il est à noter aussi que la limite de 140 caractères sur Twitter n'est imposée que dans les *tweets*. Dans la page de profil d'un individu, le nombre de caractères est de 160. On y retrouve en plus un endroit spécifique pour inscrire une adresse URL au long. Il n'y a donc pas de raison de raccourcir une adresse URL dans une page de profil. Une adresse URL raccourcie inutilement peut présenter un haut risque de contenu douteux.

Questions à vérifier

- *Est-ce qu'il est possible de vérifier l'adresse URL en entier avant de cliquer ?*
- *Est-ce que le message a un nombre de caractères limité ? Est-ce que le lien a une raison d'être raccourci ?*
- *Qui publie le lien ? Est-ce une personne de confiance ? A-t-il beaucoup d'abonnés ? Est-ce que des personnes de confiance sont abonnées à cet usager ?*
- *Le texte qui accompagne le lien en décrit-il le contenu ? Ou s'agit-il simplement d'une invitation à le suivre ?*

d. La consultation décontextualisée

Comme pour le blogue traditionnel, Twitter présente des risques que les commentaires écrits soient lus hors de leur contexte. Ce risque est accentué sur Twitter par deux particularités : le maximum de caractères et la fonction de recherche.

D'abord, comme le *tweet* ne peut comporter qu'un maximum de 140 caractères, l'usager doit aller à l'essentiel. Pour ce faire, il peut arriver qu'il omette le contexte ou les motifs qui le poussent à écrire son commentaire. Un exemple illustre bien les risques associés à la fonction de recherche. Si une entreprise désire savoir ce que les usagers

pensent de ses produits et services, elle peut inscrire son nom dans la fonction recherche. Si un employé a écrit « Travailler pour cette compagnie est pénible », la compagnie lira ce commentaire sans aucune explication ou contexte. Autre exemple : exaspéré d'avoir vu son vol repoussé, un Britannique a fait une blague noire sur Twitter au sujet de l'aéroport Robin Hood en insinuant qu'il devrait le faire exploser. Cette blague, prise très au sérieux par les autorités, lui a valu sept heures d'interrogatoire, la perte de son emploi et une amende de 1 000 Euros[104].

Ces deux caractéristiques, maximum de caractère et fonction de recherche, génèrent de grands risques de décontextualisation.

Questions à vérifier
▪ *L'information publiée est-elle confidentielle ?*
▪ *Les micromessages sont-ils médisants ?*
▪ *S'il s'agit d'humour, comprend-on bien qu'il s'agit d'une blague ? Et ce, même si le lecteur ne connaît pas personnellement l'auteur du message ?*

e. L'utilisation des messages à des fins judiciaires ou commerciales

La fonction *Retweet* augmente considérablement la persistance des informations sur Internet. Il y a donc de très haut risque qu'une fois publié, le message persiste dans le cyberespace. Le message pourrait être utilisé en preuve dans le cadre d'une procédure judiciaire.

Les conditions d'utilisation de Twitter prévoient que l'usager accorde une licence à Twitter[105]. L'usager perd la maîtrise exclusive de ce qu'il publie. Twitter se réserve le droit d'utiliser à sa guise les *tweets* à des fins commerciales. Jusqu'à maintenant, cette disposition ne semble pas avoir engendré de différends. Il existe tout de même un risque qu'un usager voit ses *tweets* servir à des fins commerciales ou publicitaires.

Question à se poser
• *L'utilisateur est-il au courant de l'appropriation des tweets par Twitter à des fins commerciales?*
• *Est-il conscient que les messages peuvent servir à des fins judiciaires?*

f. L'usurpation d'identité et l'hameçonnage

Les comptes Twitter peuvent être créés très facilement. N'est requise pour l'inscription qu'une adresse courriel valide. Un usager peut ainsi se faire passer pour une vraie personne et écrire des messages publics en son nom et ainsi causer des dommages.

---

104 BBC News South Yorkshire, "Man in Twitter bomb threat against airport loses appeal", 11 novembre 2010, http://www.bbc.co.uk/news/uk-england-south-yorkshire-11736785 (site visité le 19 décembre 2011).

105 « Vos droits », *Twitter|Conditions d'utilisation*, 18 septembre 2009, http://twitter.com/tos, (site consulté le 19 décembre 2011).

L'usurpation d'identité est aussi utilisée pour hameçonner. Les usurpateurs créent un compte au nom d'une célébrité, accompagné d'une photo de celle-ci. Ils se constituent une grande liste d'abonnés. Plusieurs sont alors tentés de *suivre* la célébrité. Cette dernière envoie alors des messages publicitaires. Ainsi, le Dalaï Lama a fait l'objet d'usurpation d'identité. Un faux compte Twitter a été créé à son nom[106]. Pour l'entreprise ou l'organisme public qui utilise Twitter, ces phénomènes impliquent de s'interroger sur les façons de rassurer ses abonnés quant à l'authenticité de son identité.

g. Les atteintes au droit d'auteur

Le risque de violation de droit d'auteur paraît faible sur Twitter. Pour ce faire, il faudrait que le tweet copié soit protégé par droit d'auteur. Or, il n'est pas certains que les 140 caractères suffisent pour produire une œuvre originale de l'esprit qui soit protégée[107].

Toutefois, un slogan publicitaire, une marque ou signe distinctif, les vers importants d'un poème ou d'une chanson pourraient faire l'objet d'une protection de droits d'auteur. Il convient d'obtenir l'autorisation avant de reproduire sur Twitter de tels contenus.

Question à vérifier
- *L'auteur du tweet qui utilise du matériel protégé a-t-il eu l'autorisation pour le faire ?*

3. Comment évaluer ces risques ?

a. L'usager a-t-il choisi des critères de confidentialité privés ?

Il est possible sur Twitter de paramétrer son compte à « privé ». Cela a pour effet de rendre les *tweets* seulement accessibles aux personnes que l'on a autorisé. En paramétrant ainsi le compte, Twitter ressemble plus à un réseau social où l'on peut choisir qui entre dans son cercle privilégié.

De paramétrer ainsi le compte d'un usager permet de réduire les risques de divulgation de renseignements personnels et d'utilisation des messages à des fins commerciales. Toutefois, paramétrer ainsi le compte n'empêche aucunement l'usager d'avoir accès à tout ce qui se trouve sur Twitter. Ainsi subsistent, avec la même intensité, les risques d'être redirigé vers du contenu inapproprié.

---

106 TECHNAUTE.CA, « Un faux Dalaï-Lama sur Twitter », *Cyberpresse*, (12 février 2009), http://technaute.cyberpresse.ca/nouvelles/internet/200902/10/01-825928-un-faux-dalai-lama-sur-twitter.php (site consulté le 19 décembre 2011).

107 *Loi sur le droit d'auteur*, L.R.C. 1985, c. C-42, art. 2.

b. L’usager est-il « suivi » par un proche ou quelqu’un de confiance ?

L’usager qui est « suivi » par un proche ou un collègue aura certainement plus tendance à faire attention à ce qu’il écrit. Les usagers savent alors que tout ce qu’ils publieront sur leur Twitter pourra être lu par leurs collègues.

c. L’usager utilise-t-il un pseudonyme ?

Le pseudonyme sur Twitter est tout à fait permis. La plupart des usagers s’identifient par leur nom, car ils utilisent Twitter comme outil d’auto-promotion. Toutefois, un usager qui veut seulement utiliser Twitter pour converser avec ses amis est plus justifié d'utiliser un pseudonyme. Ce pseudonyme a pour effet de diminuer les risques de divulgation de renseignements personnels compromettants. En effet, il devient plus difficile de compiler des informations sur un usager lorsque son nom n’est pas indiqué.

Toutefois, il convient de rappeler que le pseudonyme ne réduit en rien les risques de poursuite pour diffamation ou de sanctions criminelles pour des propos inopportuns. Il peut même parfois accentuer ces risques en générant un sentiment d’invulnérabilité.

d. L’usager est-il conscient du caractère public de Twitter ?

L’usager doit être conscient que sur Twitter, ce n’est pas seulement un cercle étendu de personnes qui ont accès à ses dires, mais bien « tout le monde». Cette conscience n’est pas nécessairement reliée à l’âge puisque même des adultes oublient ce fait.

Principalement, il s’agit de se demander si l’usager sait que « tout le monde » inclut l’employeur, les médias, les inconnus, etc.

4. Quelles sont les précautions à prendre ?

a. Informer les usagers des risques d'utilisation du micro-blogue

Twitter est accessible à tous depuis n’importe quel ordinateur relié à Internet. Il l’est aussi via un téléphone mobile relié à Internet. De plus, il est accessible aux utilisateurs de tous âges.

Twitter, contrairement aux réseaux sociaux, demande un effort de discernement constant. Comme l’information est entièrement publique, il faut être en mesure de se demander si l’information contenue dans le micromessage peut s’avérer compromettante.

Twitter demeure un outil très rapide et efficace pour l’échange d’information. Il convient de l’utiliser avec soin et prudence. Les usagers doivent être conscients des risques auxquels ils s'exposent.

b. Sensibiliser les usagers aux bonnes pratiques et comportements

Quelques bonnes pratiques peuvent être encouragées afin de minimiser les risques associés au micro-blogue.

i) La protection de la vie privée d'autrui :

Lorsqu'un utilisateur veut parler d'une autre personne, il est préférable d'identifier uniquement les individus membres de Twitter. Par exemple : « Je suis allé manger avec @YvonTremblay ».

Pour identifier les personnes qui n'utilisent pas Twitter, il est préférable de les présenter seulement par leur rôle. Par exemple, plutôt que d'écrire : « Je suis allé manger avec Jean Tremblay », il serait moins risqué d'écrire : « Je suis allé manger avec un bon ami/collègue/frère ».

Une personne qui utiliserait Twitter pour informer de ce qui se passe au sein d'une entreprise ne doit pas identifier une personne par son nom. Par exemple, « Bravo Jonathan Tremblay pour ta promotion! » pourrait être problématique. Toutefois, il est envisageable de n'utiliser que le prénom : « Bravo Jonathan pour ton succès ». Si toutefois le prénom est si peu courant qu'il identifie une personne avec trop de précision, il est préférable de ne pas la nommer du tout.

ii) La protection de ses informations :

À tout moment, il convient de se rappeler que Twitter n'est pas un outil approprié pour échanger des secrets. Le contenu est entièrement public. Même si un compte est privé, il est possible pour ses abonnés de republier le contenu et de l'associer à son auteur.

iii) Prévenir la redirection vers des contenus inappropriés :

En présence de liens raccourcis sur Twitter, il convient d'abord de se demander qui publie le lien. La page de profil d'un membre ainsi qu'un aperçu de ses *tweets* sont souvent un indice de la qualité de ses publications.

Il convient aussi de vérifier si le membre a l'habitude d'accompagner ses liens de texte. Une simple invitation à suivre un lien (« Aller voir ça, c'est génial!!! http://bit.ly/exemple ») est un indice de haut risque.

Dès lors qu'un doute subsiste, il est approprié d'utiliser une extension Bit.ly ou autre. Une extension Bit.ly est un module complémentaire que l'on peut ajouter à son client de navigation. Ce module fait en sorte que les liens raccourcis vont s'afficher dans notre navigateur en version longue.

iv) Prévenir la consultation décontextualisée :

Ce risque peut se résoudre généralement par une seule question : « Y a-t-il des chances que ce que j'écris puisse déplaire, ne serait-ce qu'à une seule personne, susceptible ou non d'utiliser Twitter ? ». Si la réponse est oui, il vaut mieux y repenser avant de publier le message. Il sera peut-être plus opportun de publier le message dans un autre réseau social ou via un autre moyen de communication.

Il est conseillé aussi d'éviter l'utilisation de l'ironie comme type d'humour. L'impossibilité de prendre connaissance du ton réel de la personne rend ce procédé humoristique très dangereux. De plus, il y a le risque que le message soit lu par des personnes qui supportent mal l'ironie.

v) Tenir compte des possibilités d'utilisation des micromessages à des fins judiciaires :

Tout ce qu'on dit sur Twitter peut être retenu contre nous. Ces micromessages peuvent éventuellement être mis en preuve devant un tribunal ou un arbitre. Il importe donc de se rappeler de bien se comporter sur Twitter. Il peut s'avérer risqué d'utiliser Twitter pour évacuer ses frustrations ou se vanter de ses « mauvais coups ».

c. « Suivre » la personne sous notre surveillance

Il convient enfin de rappeler que la précaution la plus efficace pour minimiser les risques est probablement de « suivre » par le biais de Twitter la personne qui est sous notre surveillance.

E. Les sites de notation de personnes, de services ou de produits

1. Qu'est-ce qu'un site de notation ?

Un site d'évaluation de produits et de services offre généralement au public la possibilité d'évaluer et de commenter un service reçu ou encore un bien acheté. Des sites vont également proposer d'octroyer une note aux attributs physiques d'une personne ou encore à une panoplie de biens, comme des voitures ou des animaux. La soumission d'une évaluation est facile, il suffit généralement de cliquer sur un lien, parfois nommé « *Rate this* », « *Rate My…* » et de remplir ensuite le formulaire d'évaluation.

Un des buts recherchés par ces sites est d'informer les personnes intéressées par un produit ou un service sur la qualité de ce dernier ou, à tout le moins, sur ce que les autres pensent de ce produit ou service. Les gens qui évaluent sont généralement des personnes qui ont acheté ou utilisé le bien ou le service en question. Les consommateurs qui ont accès à ces évaluations peuvent donc prendre une décision plus éclairée avant de faire un achat. Une personne qui veut se procurer une bicyclette, par

exemple, ne choisira probablement pas d'acheter la marque qui s'est méritée une centaine de commentaires négatifs. Elle choisira plutôt la marque qui a reçu des évaluations positives. De la même façon, les gens ne seront pas portés à requérir les services d'un dentiste auquel on aurait attribué plusieurs commentaires négatifs.

Les sites d'évaluation de personnes ont plutôt pour but de divertir le public en proposant d'évaluer la beauté de celles qui ont soumis leur photographie. Ces personnes seront évaluées au moyen d'une note qui est habituellement de 1 à 10. Certains sites vont ensuite proposer un classement des individus ainsi jugés les plus jolis. D'autres offrent un service de rencontre en mettant en relation un membre du site et un visiteur qui a été séduit par le membre en question.

Les modes d'évaluation des biens ou services soumis peuvent être extrêmement différents d'un site à l'autre. Certains proposent un système de notation sur une échelle de 1 à 10, d'autres attribuent cinq étoiles ou moins au bien en question. On peut aussi, dans certains cas, laisser un commentaire avec l'évaluation soumise. Généralement, les évaluations soumises sur ces sites ne peuvent pas être retirées par l'auteur lui-même. Seuls les administrateurs du site peuvent les supprimer, sur justification de la demande. De plus, certains sites permettent d'évaluer une seule fois un produit ou une personne, tandis que d'autres permettent de l'évaluer un nombre de fois indéfini.

L'adhésion à un tel site d'évaluation peut être volontaire ou non. Habituellement, les sites d'évaluation de services reçus ne sont pas basés sur une procédure d'inscription volontaire. Ce sont les personnes qui ont reçu le service qui inscrivent sur le site le nom et l'appréciation du service reçu. Par exemple, sur le site *RateMyProfessors.com*, qui évalue l'enseignement de certains professeurs, ce sont habituellement des élèves qui ajoutent les noms de professeurs à la base de données du site et non les professeurs eux-mêmes.

De la même façon, plusieurs sites de commerce électronique, comme eBay, incorporent au service de vente une évaluation des produits vendus, des vendeurs et des acheteurs. L'adhésion à cette procédure de notation n'est pas volontaire, elle est obligatoire si nous voulons faire affaire sur le site. Ces évaluations permettent ensuite de savoir si un vendeur est apprécié des autres utilisateurs du site, ou si l'acheteur avec qui nous faisons affaire n'est pas en retard lorsqu'il paie des articles.

Par contre, l'adhésion à certains types de sites d'évaluation sera totalement volontaire. Ces sites consistent généralement à évaluer les attributs physiques d'une personne (exemple : http://www.hotornot.com/) ou encore des biens en sa possession comme un animal ou une voiture (exemple : http://www.ratemyride.com/). Il suffit de soumettre une photographie qui sera ensuite publiée sur le site pour que le public l'évalue.

a. Qui fait quoi ?

i) Les usagers

Les usagers jouent un rôle fondamental dans les sites de notation. Ce sont eux qui mettent en ligne les avis et les cotes, et cela constitue le fondement même de l'existence des sites d'évaluation.

ii) Les personnes, organismes ou entreprises évalués

Tous les sites de notation ont une chose en commun, soit celle d'évaluer un objet en particulier. Dans certains cas, ce sont des personnes, dans d'autres des services et, pour quelques autres, ce sont des biens. Dans tous les cas, ces « objets » sont « notés » par les usagers des sites.

Une personne peut décider de mettre en ligne une photo ou une vidéo d'elle-même pour qu'elle soit notée par les autres. Dans ce cas, l'usager sera la personne évaluée. Elle peut également mettre en ligne la photo de quelqu'un d'autre – notamment par le biais de sites comme Dontdatehimgirl.com. Dans ce cas, la personne n'a pas décidé de se retrouver en ligne. C'est d'ailleurs le processus normal pour les sites de notation. Certains sont dédiés aux travailleurs ou aux professionnels, notamment les dentistes, médecins, avocats, comptables, etc.

Aussi, il existe des sites permettant aux employés d'évaluer leur entreprise, et ce, anonymement. D'autres sites évaluent les restaurants, la qualité de la nourriture, le service et l'expérience qu'on y a vécue.

iii) Les sites de notation

Les sites de notation offrent le cadre dans lequel on peut ajouter des évaluations et des informations sur un « objet » donné. La qualification de ces sites n'est pas claire. Sont-ils des éditeurs ou des hébergeurs ? La responsabilité qui en découlera sera bien différente et les enjeux sont majeurs vu la nature controversée des sites de notation. Par exemple, un site qui participe à l'édition de contenu en proposant des critères et catégories, ou en proposant des réponses pré-rédigées, pourrait être plus qu'un simple hébergeur et être qualifié d'éditeur. Par contraste, le site de notation qui laisse aux usagers le soin de noter à leur guise pourra plus aisément être traité au regard de la loi comme un intermédiaire de type « hébergeur ».

b. Utilisation des sites de notation

Les sites de notation sont un instrument privilégié pour les clients quand vient le temps de donner leur opinion sur les biens et services reçus d'une entreprise ou d'un organisme public.

2. Quels sont les risques associés aux sites de notation ?

a. La manipulation de l'information et le caractère erroné de celle-ci

Les sites d'évaluation de personnes, de services ou de produits peuvent être manipulés par des gens qui désirent donner une bonne ou une mauvaise note à un produit ou à une entreprise. Par exemple, il est facile pour les amis d'un individu d'aller sur un site d'évaluation de photographies où ce dernier s'est inscrit et de lui attribuer des dizaines de notes parfaites pour augmenter son évaluation. De la même façon, certains sites de commerce électronique étant basés sur la réputation des commerçants, il peut être tentant de publier une évaluation pour soi-même ou pour des amis dans le but d'embellir un profil. Un vendeur qui désire frauder, par le biais d'un site de vente aux enchères, pourrait donc se faire attribuer des évaluations positives par ses amis afin d'attirer la confiance des consommateurs.

De plus, les évaluations sur ces sites ne représentent pas toujours fidèlement la satisfaction des gens face à une transaction. Par exemple, sur un site comme eBay, où les cocontractants s'évaluent mutuellement après une transaction, certains peuvent craindre de donner une mauvaise évaluation à la personne avec qui elles ont fait affaire de peur d'en recevoir une en retour par vengeance. Le vendeur d'un article pourrait, suite à la publication d'un commentaire négatif de la part de l'acheteur, publier lui aussi un commentaire mentionnant la mauvaise foi de l'acheteur, même si celui-ci a rempli ses obligations.

Questions à vérifier

- *Est-il possible de soumettre plusieurs évaluations provenant de la même personne ?*
- *Le mécanisme d'évaluation fait-il en sorte qu'une personne peut craindre de subir des représailles suite à une évaluation négative ?*

b. Les atteintes à la réputation et à la vie privée

Il est possible d'entacher la réputation de quelqu'un en évaluant le service ou le produit qu'elle fournit. En effet, le but du service d'évaluation est de noter un service, un produit ou une personne. Chaque évaluation négative atteindra donc nécessairement la réputation de la personne qui fournit le bien ou le service, et c'est habituellement l'objectif poursuivi pour éviter que d'autres acheteurs ou vendeurs fassent affaire avec un cocontractant négligent.

Par contre, il faut éviter de faire une évaluation négative qui rapporterait des faits mensongers ou encore des faits véridiques rappelés inutilement dans le seul but de nuire. Par exemple, dire d'un auteur qu'il est un criminel sur un site d'évaluation et de vente de livres peut attenter à sa réputation.

Sur le site *Ratemyprofessors.com*, une liste des choses à faire et à ne pas faire est disponible pour diriger les élèves voulant inscrire un commentaire concernant leurs professeurs[108] :

DOs :

- *Be honest.*
- *Be objective in your assessment of the professor.*
- *Limit your comments to the professor's professional abilities. Do not get personal.*
- *Proof your comments before submitting. Poor spelling WILL NOT cause your rating to be removed; however, poor spelling may result in your rating being discredited by those who read it.*
- *Leave off your Name, Initials, Pseudo Name, or any sort of identifying mark when posting.*
- *Refer to the Rating Categories to help you better elaborate your comments.*
- *Remember that negative comments that still offer constructive criticism are useful. Comments that bash a professor on a personal level are not.*
- *Submit helpful comments that mention professor's ability to teach and/or communicate effectively, course load, type of course work and course topics.*

DO NOTs :

- *State something as a fact if it is your opinion.*
- *Post a rating if you are not a student or have not taken a class from the professor.*
- *Post ratings for people who do not teach classes at your college or university.*
- *Input false course or section codes for a class that does not exist.*
- *Rate a professor more than once for the same class.*
- *Make references to other comments posted.*
- *Professors: Do not rate yourselves or your colleagues.*[109]

Questions à vérifier

- *Le participant est-il amené à dévoiler des renseignements personnels sur lui-même ou sur une autre personne ?*
- *Est-ce que le site d'évaluation de personnes, de produits ou de services offre une méthode pour dénoncer le contenu inapproprié ?*
- *Est-il possible de soumettre plusieurs évaluations provenant de la même personne ?*

---

108 « Posting Guidelines », RateMyProfessors.com, en ligne : http://www.ratemyprofessors.com/rater_guidelines.jsp (site consulté le 19 décembre 2011)

109 « Posting Guidelines », RateMyProfessors.com, en ligne : http://www.ratemyprofessors.com/rater_guidelines.jsp (site consulté le 19 décembre 2011)

c. La divulgation de renseignements personnels

La divulgation de renseignements personnels sur des sites tels ceux proposant un service de rencontres (adresse de courriel, numéro de téléphone, adresse) peut donner lieu à l'envoi de menaces ou à du harcèlement.

Une personne peut également publier une évaluation qui révèle des informations personnelles sur elle-même ou sur un tiers. La plupart des sites interdisent de mettre en ligne ces informations et les suppriment lorsqu'une telle publication est portée à leur connaissance.[110]

Questions à vérifier
• *Le participant est-il amené à dévoiler des renseignements personnels sur lui-même ou sur une autre personne ?*
• *Est-ce qu'il y a présence de modération sur le site ?*

d. L'utilisation non autorisée de l'image

Sur certains sites d'évaluation, il est possible de publier la photographie de la personne évaluée. Cette publication peut être faite avec l'accord de la personne concernée ou sans son consentement, ce qui peut constituer une utilisation non autorisée de son image.

Question à vérifier
• *Est-il possible de publier la photographie d'une personne sur le site d'évaluation ? Si oui, la publication des photographies a-t-elle été autorisée ?*

e. La responsabilité pour les informations diffusées

La question de savoir qui est responsable de l'information se retrouvant sur un site d'évaluation de personnes, de produits et de services reste entière. Ces sites se déchargeront habituellement de la responsabilité du contenu publié par les participants mais, s'ils sont avertis qu'un propos illicite se retrouve sur le site, ils ont l'obligation de réagir et de le retirer, si le caractère illicite se confirme.

Par contre, pour tenir responsable la personne qui a écrit un message inapproprié, le plus grand défi est de la retracer. En effet, dans la plupart des cas, les sites d'évaluation ne demandent aucune information permettant d'identifier la personne qui veut évaluer un produit. Certains sites préviennent l'usager que son adresse IP sera enregistrée. Pour retracer une personne qui aurait mis en ligne un commentaire menaçant, par exemple, il faudrait obtenir cette adresse IP enregistrée par le site et l'heure de la publication.

---

110 Sarah COLOMBO, « Trade association proposed to represent rating websites », *Online Journalism Review*, 10 mai 2007, en ligne : http://www.ojr.org/ojr/stories/070508colombo (site consulté le 19 décembre 2011).

Ensuite, il faut vérifier à qui appartenait cette adresse à cette heure précisément auprès du fournisseur d'accès à Internet. Même après ces démarches, il n'est pas garanti que l'identité de la personne soit retracée.

> ***Questions à vérifier***
> - *Est-ce qu'il y a des mécanismes de surveillance du contenu sur le site en question ?*
> - *Les interventions anonymes sont-elles permises ?*
> - *Est-ce que le site Internet sauvegarde des informations personnelles permettant de retracer une personne ? Si oui, le site prévient-il les usagers de cette sauvegarde ?*

3. Comment évaluer ces risques ?

a. L'objet de l'évaluation et les fonctions offertes par le site

Sur les sites d'évaluation, on peut noter des biens, des personnes, des services, etc. Les risques ne sont pas les mêmes, dépendant de l'objet de l'évaluation. Par exemple, un site qui propose d'évaluer les attributs physiques d'une personne risque davantage de poser des problèmes de droit à l'image qu'un site qui permet d'apprécier la qualité de l'histoire d'un livre de poche.

De plus, les fonctions offertes sur le site ont un grand impact sur les risques qui y sont associés. Un site qui offre de laisser un commentaire, en plus d'une évaluation chiffrée, ouvre une porte à des propos diffamants à l'égard d'une personne. Par contre, un site qui n'offre que l'évaluation chiffrée de 1 à 10 pose moins de risques car il ne laisse pas la possibilité de publier de commentaires personnels.

> ***Questions à vérifier***
> - *Quel type d'évaluation retrouve-t-on sur le site Internet ?*
> - *Est-il possible de joindre un commentaire à une évaluation ou est-ce seulement une évaluation chiffrée ?*

b. La présence de modération

Certains sites d'évaluation de personnes, de produits et de services préfèrent mettre en place un mécanisme de modération pour s'assurer que les évaluations des usagers ne comportent pas de contenu inapproprié. Cette modération peut se faire avant que l'évaluation soit publiée ou après.

Lorsque la modération est faite *a priori,* les évaluations soumises ne seront pas immédiatement mises en ligne une fois complétées. Il y aura plutôt un délai de quelques jours avant que l'on puisse les consulter. Cette procédure est utilisée, entre autres, par le site Amazon, qui se réserve un délai de cinq à sept jours avant la publication des évaluations et des commentaires.

La modération peut se faire également *a posteriori*, c'est-à-dire après que l'évaluation soit en ligne. Dans la plupart des cas, les sites qui modèrent avant la publication vont également le faire après puisqu'il est toujours possible qu'un contenu inapproprié ait été publié par erreur. Habituellement, ce type de modération se fait grâce aux utilisateurs du site. Chaque évaluation sera associée à un lien, généralement nommé « *Flag this rating* », invitant à dénoncer le contenu s'il paraît illicite. Lorsqu'un commentaire est signalé, un modérateur du site l'analyse et décide s'il faut le retirer.

D'autres sites prévoient des sanctions pouvant être prises, en cas de récidive par les membres ne respectant pas les règles de conduite mises en place.

Questions

- *Est-ce que le site d'évaluation est modéré ? Si oui, de quelle façon ? Cela se fait-il avant ou après la publication d'une évaluation ?*

c. Le caractère anonyme ou non des participants

Sur un site où l'anonymat est totalement garanti, la publication de propos susceptibles d'être mensongers est plus facile que sur un site où il faut s'identifier. D'un autre côté, un site exigeant de s'identifier pour publier un commentaire risquerait de diffuser des informations trompeuses ou erronées puisque les gens pourraient se retenir de dire vraiment ce qu'ils savent par crainte de représailles.

Questions à vérifier

- *Est-ce que les participants communiquent dans l'anonymat ?*
- *Est-ce que les participants utilisent des pseudonymes ?*
- *Est-ce qu'il y a des restrictions quant aux personnes pouvant publier un commentaire ?*

d. La possibilité de laisser plusieurs évaluations pour un même produit ou une même personne

Certains sites permettent à un utilisateur de laisser une seule évaluation pour un produit ou une personne. Cela réduit le risque que l'évaluation d'un produit ou d'un service d'une personne soit manipulée par ses amis qui veulent lui donner une bonne note. Par exemple, si plusieurs commentaires positifs existent pour un restaurant sur un site où il n'existe aucune limite de commentaires, ces derniers pourraient perdre de leur force probante puisqu'on pourra se demander s'ils émanent ou non de véritables clients témoignant de leur véritable expérience.

Ce contrôle peut se faire en limitant le nombre de commentaires possibles pour une adresse IP donnée. En effet, si plusieurs évaluations sont envoyées par la même adresse IP dans une courte période de temps, les modérateurs supprimeront ces messages.

Question à vérifier

- *Est-ce que le site d'évaluation empêche que plusieurs évaluations proviennent de la même personne ?*

4. Quelles sont les précautions à prendre ?

a. Établir des conseils d'écriture pour les évaluations

Pour éviter la mise en ligne de contenu inapproprié, il peut être prudent pour un site d'évaluation de mettre à la disposition des usagers des conseils d'écriture. Ces conseils informent les participants des pratiques tolérées et celles qui ne le sont pas. Lorsque ces conseils se retrouvent déjà sur le site, il est important d'en prendre connaissance pour éviter qu'un commentaire publié soit retiré.

b. Mettre sur pied un processus de vérification du contenu

Que ce soit par les utilisateurs ou par les administrateurs du site, il serait prudent de mettre sur pied une procédure de vérification du contenu. La loi québécoise prévoit que les responsables de sites dans lesquels se retrouvent des documents placés par les usagers n'ont pas l'obligation d'exercer une surveillance.

Une procédure de vérification du site par les utilisateurs peut être une bonne alternative. Il s'agit d'inviter les gens à dénoncer un contenu illicite, par une méthode facile offerte par le site. En plus de disposer d'un plus grand nombre de vérificateurs puisque tous les visiteurs peuvent dénoncer un contenu, cette méthode n'engagera pas indûment la responsabilité du site, à moins qu'il ait été averti de l'existence d'un contenu illicite et qu'il n'ait pas agi promptement pour le vérifier.

c. Établir une politique d'utilisation du site

Le site d'évaluation de personnes, de produits ou de services doit établir des règles quant à l'utilisation de son service. Il doit fixer les conditions de la participation d'un internaute au site[111]. Il pourrait, entre autres, interdire les propos à caractère sexuel, raciste ou violent. Si les conditions d'utilisation ne sont pas respectées, le site peut se réserver le droit de supprimer le commentaire ou de fermer le compte de la personne mal intentionnée.

d. Informer les participants des risques liés à l'usage des sites de notation

Il est important de sensibiliser les usagers aux risques auxquels ils s'exposent en utilisant les sites d'évaluation ou de notation, que ce soit pour la préservation de leurs

---

111 Anne-Sophie POGGI, « Sites marchands participatifs : 3 règles pour éviter le hors piste », *Le journal du Net*, 11 septembre 2007, http://www.journaldunet.com/ebusiness/expert/14224/sites-marchands-participatifs---3-regles-pour-eviter-le-hors-piste.shtml

renseignements personnels ou pour éviter de voir reconnaître responsable d'une situation.

F. Les sites Wikis

1. Qu'est-ce qu'un site Wiki ?

Un Wiki est « un type particulier de site Web permettant à une communauté de créer et de modifier collectivement un contenu publié en ligne »[112]. Le terme « *Wiki* » est un mot dérivé de l'expression hawaïenne *wikiwiki* qui signifie « vite »[113].

Les Wikis remplissent une multitude de fonctions ; ils sont utilisés comme site d'information en ligne, roman ou encore document collaboratif sur un lieu de travail. Contrairement à un blogue - qui est davantage le résultat du travail d'un seul individu - un site Wiki fait appel à la collectivité. Les visiteurs sont appelés à intervenir sur le site en ajoutant ou en corrigeant des informations inexactes ou incomplètes.

Les Wikis se distinguent par leur aspect collectif et collaboratif. Leur caractéristique fondamentale est que le simple visiteur du site peut en modifier le contenu. Les Wikis n'utilisent pas une hiérarchie formelle, mais sont plutôt structurés de façon horizontale (hyperliens entre les pages du site et avec des pages externes). Ils constituent une des figures exemplaires du phénomène du Web 2.0. Il existe des Wikis publics comme Wikipédia et d'autres privés ou à accès restreint où un mot de passe et un nom d'usager sont nécessaires[114].

L'utilisation des sites Wikis est souvent encadrée par des règles. Une plus grande liberté d'effectuer une modification de contenu ne signifie pas une absence de contrôle. On interdira généralement le plagiat d'une œuvre protégée ou encore les propos insultants. Certains sites restreignent également les paramètres de modification des articles aux seuls membres enregistrés qui auront fourni leur véritable identité. Pour plus de sécurité, chaque modification est conservée dans une base de données. Si une personne mal intentionnée efface des articles, il sera alors possible de les récupérer. On peut voir l'historique de ces modifications en cliquant sur le lien « Historique » du site Wiki.

---

112 Lucie AUDET, « Wikis, Blogues et Web 2.0, Opportunités et impacts pour la formation à distance », *Le Réseau d'enseignement francophone à distance du Canada (REFAD)*, mars 2010, en ligne : http://www.refad.ca/nouveau/Wikis_blogues_et_Web_2_0.pdf .

113 Office québécois de la langue française, « site Wiki », en ligne : http://www.granddictionnaire.com/BTML/FRA/r_Motclef/index800_1.asp (site consulté le 19 décembre 2011).

114 Lucie AUDET, « Wikis, Blogues et Web 2.0, Opportunités et impacts pour la formation à distance », *Le Réseau d'enseignement francophone à distance du Canada (REFAD)*, mars 2010, en ligne : http://www.refad.ca/nouveau/Wikis_blogues_et_Web_2_0.pdf (consulté le 19 décembre 2011).

Pour créer un site Wiki, il faut posséder un logiciel de gestion de sites Wikis comme MediaWiki[115], TWiki[116] et MoinMoin[117]. Si le site Wiki est déjà créé et que l'on veut apporter certaines modifications, cela ne demande aucun logiciel en particulier ; il suffit de se rendre sur la page en question et de cliquer sur le lien « Voir le texte source » ou « Modifier ». En comparaison, la modification d'un site Wiki est un peu plus difficile que la modification d'un blogue. En effet, pour éditer un texte « Wiki », il faut utiliser le langage Wikitexte, qui ressemble à du langage HTML – le langage des pages Web régulières, en version simplifiée. Il faut alors mettre certains mots entre crochets ou ajouter des expressions devant des mots pour faire la mise en forme du texte. Cependant, pour les fonctions de base, comme mettre un mot en caractère accentué, des icônes, semblables à celles qui se retrouvent dans un logiciel de traitement de texte, facilitent le travail[118].

Les articles publiés sur un site Wiki sont habituellement libres de droit, la licence de documentation libre GNU[119] étant généralement utilisée. Une fois en ligne, les utilisateurs ayant les autorisations nécessaires peuvent donc reprendre l'article et le modifier à leur guise. Toute personne connectée à Internet peut agir, sans aucune formalité d'inscription[120]. Ainsi, tout utilisateur enregistré peut créer un nouvel article, puis tout internaute peut éditer cet article, en ajoutant, supprimant ou modifiant du contenu.

a. Qui fait quoi ?

i) Les lecteurs

Les lecteurs sont ceux qui se rendent sur les sites Wikis afin de consulter les informations qui s'y trouvent. Ainsi les utilisateurs se rendront sur Wikipédia pour obtenir de l'information sur un sujet quelconque, iront sur Wikitravels pour découvrir une destination voyage, etc. Le lecteur n'édite pas les informations qu'il lit, il peut le faire, mais il devient à ce moment un acteur actif du monde des Wikis.

---

115 « Welcome to **MediaWiki.org** », MediaWiki, en ligne : http://www.mediawiki.org/wiki/ MediaWiki/ (site consulté le 19 décembre 2011).

116 TWiki, en ligne : http://twiki.org/ (site consulté le 19 décembre 2011).

117 MoinMoin, en ligne : http://moinmo.in/ (site consulté le 19 décembre 2011).

118 Sébastien BLONDEEL, *Wikipédia : comprendre et participer*, coll. « Connectez-moi ! », Paris, Éditions Eyrolles, 2006.

119 « GNU Operating System », en ligne: http://www.gnu.org/copyleft/fdl.html (site consulté le 19 décembre 2011).

120 Louise-Marie RIOUX SOUCY, « Wikipédia resserre les rênes », *Le Devoir*, 7 décembre 2005, en ligne : http://www.ledevoir.com/2005/12/07/97136.html (site consulté le 19 décembre 2011).

ii) Les éditeurs / les usagers

Les éditeurs sont les acteurs qui participent à la construction de sites Wikis. Ce sont eux qui créent le contenu des pages Web et qui les modifient au fil du temps. De plus, sur Wikipédia, des informations sur les utilisateurs sont disponibles (comme l'heure, la date et le nombre de modifications) et sont accessibles au public grâce à la page des « contributions de l'utilisateur ». Selon Wikipédia, le compte d'utilisateurs ne sera jamais supprimé. « La suppression de données spécifiques d'un compte utilisateur est laissée à la discrétion de la politique de suppression du wiki où le compte est actif »[121].

iii) Les administrateurs/les développeurs

De nombreux débats d'idées naissent tous les jours sur Wikipédia, ainsi que des conflits d'autres natures, tels que les enjeux de vie privée ou de propriété intellectuelle. Le site a donc mis en place un système gradué de résolution des conflits : principe de bonne foi, page de discussion, médiation informelle, médiation formelle, arbitrage[122]. Ce système permet de solutionner la plupart des différends, sans avoir recours aux tribunaux.

Le site Wikimedia a mis en place un système d'administrateurs qui font un travail d'administration sur les serveurs de Wikimedia[123]. Ce sont eux qui retirent les éléments qui ont été dénoncés comme portant atteinte aux droits ou comme violant les règles des sites Wikis, notamment par rapport au droit d'auteur.

Il peut arriver que les administrateurs de Wikipédia suppriment définitivement certaines parties de l'historique d'un article, dans les cas de diffamation, par exemple, ou lorsqu'une information privée a été mise en ligne (par exemple, un numéro de téléphone). Comme l'historique peut être consulté par tout internaute, la diffamation ou l'atteinte à la vie privée pourrait continuer à causer du dommage si l'historique n'était pas expurgé de son contenu litigieux.

iv) Les hébergeurs

Les hébergeurs sont ceux qui permettent aux sites Wikis de voir le jour. Pensons aux Wikis gratuits qui offrent de l'hébergement: MediaWiki, Wikispaces, PBwiki, Wetpaint, Wikia, BluWiki et XWiki.

---

121 « Information sur les utilisateurs – Politique de confidentialité », Wikimedia Foundation, en ligne : http://wikimediafoundation.org/wiki/Politique_de_confidentialit%C3%A9#Information_sur_les_utilisateurs (site consulté le 19 décembre 2011)

122 « Wikipedia : Dispute resolution », Wikipédia, en ligne : http://en.wikipedia.org/wiki/Wikipedia:Dispute_resolution (site consulté le 19 décembre 2011)

123 « System administrators », Wikimedia, en ligne : http://meta.wikimedia.org/wiki/Developers (site consulté le 19 décembre 2011)

L'hébergeur ne crée pas de contenus à proprement parler. Il « héberge » le contenu que les utilisateurs créeront dans les pages Web. Cela est d'autant plus vrai avec les pages Wikis où les usagers sont au cœur de la création du matériel disponible.

b. Utilisation des sites wikis

Les sites Wikis ont plusieurs utilisations possibles en entreprise.

- Contribution à l'élaboration de documents de référence sur un sujet

La contribution à l'élaboration de documents est l'usage le plus courant des Wikis. Le site est alors utilisé pour construire des répertoires sur un thème en particulier ou encore des portails de gestion de connaissances de groupes.

- La recherche dans les sources des sites Wikis et l'évaluation de leur valeur ou de leur pertinence[124]

Les Wikis constituent une source documentaire importante. Ils doivent toutefois être utilisés en conservant un sens critique quant à la pertinence et à la qualité des informations qu'on y trouve.

- Élaboration collaborative de documents

Les sites tels que Wikipédia permettent de créer des pages d'information, ou de modifier celles qui existent déjà. Les Wikis peuvent être complètement publics, permettant à n'importe quel internaute d'en modifier le contenu, ou privés, ce qui peut être pratique dans le cas d'un projet d'équipe. Le contenu des wikis peut être sous plusieurs formats : textes, images, vidéo, audio, etc.

Les Wikis offrent de multiples possibilités, par exemple :
- Les usagers peuvent annoter directement les documents sur le Wiki;
- Les usagers peuvent collaborer sur des travaux d'équipe. Le Wiki permet de toujours travailler sur la version la plus récente du document.
- Les usagers peuvent écrire, réviser et soumettre leurs travaux. Ils peuvent même documenter leurs démarches sur le Wiki en publiant leurs sources documentaires au fur et à mesure que leurs recherches avancent. Puisque le Wiki enregistre automatiquement chaque modification faite au document, il est possible de voir son évolution.
- Les usagers peuvent utiliser les Wikis pour compiler des données ou partager les résultats de leurs recherches. Il leur est ainsi possible de retrouver leur travail de n'importe quel endroit où ils ont l'accès à Internet.

---

124 Lucie AUDET, « Wikis, Blogues et Web 2.0, Opportunités et impacts pour la formation à distance », *Le Réseau d'enseignement francophone à distance du Canada (REFAD)*, mars 2010, en ligne : http://www.refad.ca/nouveau/Wikis_blogues_et_Web_2_0.pdf (site consulté le 19 décembre 2011)

Il existe d'autres utilisations pour les entreprises[125]. Par exemple :
- échange et discussions pour de nouvelles idées et nouveaux projets;
- organisation d'évènements;
- calendrier des projets;
- compte rendu de réunions;
- partage des fichiers et documents de travail;
- base de données des contacts;
- politiques.

2. Quels sont les risques associés aux sites Wikis ?

En général, les administrateurs d'un site Wiki comptent sur le bon sens et la responsabilité des visiteurs pour réguler le site. Ceux-ci doivent, s'ils trouvent un article faux ou inapproprié, le corriger ou le supprimer. Par contre, il y a parfois des failles dans ce système. Il est donc important d'examiner les risques que peut engendrer l'utilisation d'un site Wiki.

a. Les informations inexactes ou contrôlées

Le risque que des informations inexactes se retrouvent dans un site Wiki est grand. Dans un site Wiki où les gens collaborent pour écrire un roman, le risque est moins important puisque c'est de la fiction. Par contre, pour prendre l'exemple de Wikipédia, qui met en ligne une encyclopédie modifiable par tous, les personnes qui écrivent des articles ne sont pas tous des professionnels du domaine. Certaines personnes peuvent, par malveillance ou encore par ignorance, rapporter des informations inexactes qui se retrouvent sur le site. D'un autre côté, on peut y retrouver de l'information très pertinente écrite par des spécialistes ou des gens très bien renseignés. Il convient donc d'être prudent lorsque nous consultons ce genre de sites Internet.

Un autre risque relié aux sites Wikis est de voir l'information contrôlée par des gens ou compagnies en quête de publicité. Wikipédia peut être modifié par tous et de façon anonyme. Certains articles peuvent être utilisés pour mettre en valeur une compagnie ou une personne, contrevenant ainsi au « *neutral point of view* » préconisé par le site. Les auteurs intéressés à valoriser un article jouissent alors de la crédibilité et de l'apparence de neutralité de Wikipédia.

Compte tenu de la popularité de Wikipédia et de la crédibilité que les internautes lui accordent, il va de soi que les personnalités publiques et les compagnies ont intérêt à vérifier ce que le site affirme à leur sujet. Il peut être tentant de faire modifier ou de modifier soi-même l'article qui nous concerne.

---

[125] « Le Wiki en entreprise », en ligne : http://www.commentcamarche.net/faq/9699-le-wiki-en-entreprise#comprendre-les-usages-du-wiki-en-entreprise (site consulté le 19 décembre 2011).

Cette attitude est mal vue sur Wikipédia, mais même le co-fondateur Jimmy Wales n'a pu s'empêcher de retoucher quelques données peu flatteuses de sa biographie. Il aurait changé sa propre biographie quelque dix-huit fois au courant de l'année 2005[126].

D'ailleurs, les gens œuvrant en relations publiques seraient fréquemment bloqués par Wikipédia, lorsqu'ils tentent de modifier les articles concernant les produits ou l'entreprise qu'ils représentent[127].

Dans le contexte politique, la possibilité pour quiconque de modifier des articles sur Wikipédia devient un enjeu d'une grande importance. Dans les 24 heures précédant la nomination de Sarah Palin comme colistière de John McCain en août 2008, l'article dédié à la biographie de celle-ci a été modifié quelques 30 fois par un éditeur œuvrant sous le pseudonyme de « Young Trigger ». Cette personne anonyme bonifiait l'image de Palin, indiquant notamment sa forte popularité comme gouverneure, rehaussant ses accomplissements en tant que maire de Wasilla et la qualifiant de politicienne d'une intégrité éblouissante (*eye-popping integrity*)[128].

Questions à vérifier

- *Le wiki est-il public ou privé ? Le fait qu'un wiki soit public ou privé influence sur l'ampleur du risque.*
- *Est-ce que l'information se retrouvant sur le site Wiki est présentée comme étant fiable ou est-ce de la fiction ?*
- *Qui sont les gens participant au site Wiki ? Sont-ils anonymes ou identifiables ?*
- *Quel est le sujet de l'article qui nous intéresse ? Est-ce que l'article est susceptible d'être contrôlé par une personne ou une compagnie ?*

b. Les atteintes à la réputation, la propagande haineuse et les menaces

Le risque d'atteinte à la réputation est grand sur les sites Wiki et l'actualité en déborde d'exemple. En effet, lorsque des articles (comme des biographies) sont rédigés, les auteurs peuvent se tromper sur certaines informations, rappeler inutilement des moments de la vie de quelqu'un sans motif légitime, ou alors inventer des faits par rapport à une personne. En effet, la facilité d'écrire ou de modifier un article sur un site

---

126 Marie-Ève MORASSE, « Wikipédia : le fondateur change sa propre bio », *Technaute.ca*, 20 décembre 2005, en ligne : http://technaute.cyberpresse.ca/nouvelles/200512/20/01-16400-wikipedia-le-fondateur-change-sa-propre-bio.php (site consulté le 19 décembre 2011).

127 Nancy GOHRING, « Microsoft said to offer payment for Wikipedia edits - *It raises questions on the ethics of a company paying someone to edit entries*», Computer World, 23 janvier 2007, en ligne : http://www.computerworld.com/s/article/9008842/Microsoft_said_to_offer_payment_for_Wikipedia_edits (site consulté le 19 décembre 2011).

128 Noam COHEN, « Don't like Palin's Wikipedia Story ? Change it », *The New York Times*, 31 août 2008, en ligne : http://www.nytimes.com/2008/09/01/technology/01link.html?ex=1378008000&en=2690a3850cb270d0&ei=5124&partner=permalink&exprod=permalink (site consulté le 19 décembre 2011).

Wiki ainsi que la grande diffusion du message illicite peut rendre ce moyen d'expression attrayant.

Il est également possible sur des sites Wikis de faire de la propagande haineuse envers un groupe de la société. Que ce soit par des propos racistes insérés dans un texte ou encore un déni d'événements historiques tel l'Holocauste, il est facile de propager ces messages haineux et punis par la loi sur Internet. Au même titre que pour un blogue, des gens pourraient écrire des menaces ou des propos dénigrants concernant une personne ou un groupe de personnes sur un site Wiki.

Les sites Wikis prohibent la diffusion de contenus diffamatoires ou insultants. Le phénomène y est souvent qualifié de vandalisme virtuel. Toutefois l'interdiction n'est pas toujours respectée.

Par exemple, le site Wikipédia est supposé fournir des contenus objectifs (à la différence d'un Wiki d'écriture de roman, par exemple). Or, la grande difficulté est que les contributeurs peuvent agir anonymement car seule l'adresse IP est conservée et les informations ne sont validées par aucune autorité reconnue. Puisque tout le monde peut intervenir sur Wikipédia et qu'aucun contrôle *a priori* n'est effectué (sauf exception), il existe un risque de contenu illicite.

Certains articles rédigés sur Wikipédia s'apparentent aux commentaires publiés sur un blogue public sans contrôle *a priori.* En général, le site Wiki effectuera un contrôle *a posteriori*, si une plainte est déposée. Toutefois, le risque demeure que des erreurs majeures ou malveillantes persistent sur le site pour une durée indéterminée.

De nombreuses informations erronées peuvent se retrouver sur les pages de Wikipédia, que ce soit de façon innocente ou mal intentionnée. Le plus souvent, ces erreurs demeurent en ligne pour de très courts laps de temps[129]. Par exemple, le 20 janvier 2009, les sénateurs américains Edward Kennedy et Robert Byrd ont été annoncés comme étant décédés, ce qui s'est avéré un canular. Ces erreurs sont demeurées respectivement cinq et quatre minutes sur Wikipédia avant d'être corrigées[130].

Dans des cas beaucoup plus exceptionnels, les erreurs demeurent en ligne pour une plus longue période. Cela peut causer des dommages plus importants.

---

129 Voir par exemple l'étude menée en 2007 concernant les articles portant sur les sénateurs américains : Gregory KOHS, « Wikipedia Vandalism Study – US Senators », *Wikipedia Review*, 5 octobre 2008, en ligne : http://wikipediareview.com/blog/20081005/wikipedia-vandalism-study-us-senators/ (site consulté le 19 décembre 2011).

130 Ben PERSHING, « Kennedy, Byrd the Latest Victims of Wikipédia Errors », *The Washington Post*, 21 janvier 2009, en ligne : http://voices.washingtonpost.com/capitol-briefing/2009/01/kennedy_the_latest_victim_of_w.html (site consulté le 19 décembre 2011).

Il peut donc y avoir des problèmes de crédibilité, de vandalisme et de diffamation sur un site encyclopédique de référence dont les contenus sont générés par les utilisateurs. Wikipédia a d'ailleurs resserré ses normes de création de contenus, obligeant les créateurs de nouveaux articles à s'enregistrer[131]. Cette mesure a cependant été considérée par certains comme insuffisante ou inutile.[132] En effet, l'enregistrement d'un compte sur Wikipédia ne demande pas de fournir une adresse de courriel valide. On ne garantit donc pas la responsabilité de l'éditeur, et les modifications peuvent toujours être effectuées par n'importe quel internaute.

> ***Questions à vérifier***
> - *Est-ce que l'article contient des informations sur la vie de quelqu'un ?*
> - *Est-ce qu'il y a vérification, par les administrateurs du site, du contenu qui est publié ?*

c. Les contenus à caractère pornographique ou autrement inappropriés

De l'information ou des images à caractère pornographique peuvent se retrouver sur des sites Wikis. En effet, puisqu'on peut ajouter du contenu à notre guise, certains peuvent faire des modifications non appropriées, par exemple mettre en ligne des photographies obscènes. Il est donc possible de retrouver de telles images dans un article qui peut être anodin au premier abord.

De plus, certains sites Wikis ont, comme finalité, de présenter du contenu à caractère pornographique ; par exemple, des histoires auxquelles plusieurs personnes peuvent collaborer. Ces pages sont plus faciles à repérer puisqu'elles sont affichées comme telles. Les chances d'y être exposé involontairement sont donc plus faibles.

Ce matériel ne convient généralement pas à plusieurs publics, mais il n'est pas illicite. Par contre, il est possible de retrouver du contenu illégal sur un site Wiki.

> ***Question à vérifier :***
> - *Quel est le sujet du site Wiki en question ? Est-ce que le sujet convient au public qui est visé ?*

d. Les atteintes au droit d'auteur et l'utilisation non autorisée de l'image

Lorsque des photographies sont présentes sur un site, cela peut constituer une atteinte au droit à l'image, si la personne représentée n'a pas autorisé sa publication. C'est le cas

---

131 Louise-Maude RIOUX SOUCY, « Wikipédia resserre les rênes », *Le Devoir*, 7 décembre 2005, en ligne : http://www.ledevoir.com/2005/12/07/97136.html (site consulté le 19 décembre 2011).

132 Voir Anita RAMASASTRY, « Is an online Encyclopedia, such as Wikipedia, Immune from Libel suits ? », *FindLaw*, 12 décembre 2005, en ligne : http://writ.news.findlaw.com/ramasastry/20051212.html (site consulté le 19 décembre 2011)

si un site Wiki présente la biographie d'une personne et qu'on y insère sa photographie sans sa permission.

De plus, le participant au site Wiki peut emprunter des œuvres que l'on retrouve sur d'autres sites Internet ou ailleurs. Cet emprunt peut se faire pour les images mais aussi pour toute autre oeuvre, que ce soit des textes, des chansons, etc. soulevant alors des questions quant au droit d'auteur. En effet, pour publier une œuvre dont on ne détient pas les droits, il faut obtenir la permission de l'auteur en vertu de la *Loi sur le droit d'auteur*.

Lorsqu'on établit des liens hypertextes, il faut également s'assurer de respecter le droit d'auteur. Des techniques consistant à reproduire le site à l'intérieur du site Wiki (*framing*) ou encore à copier la banque de liens hypertextes d'un autre site peuvent s'avérer risquées.

Les articles publiés sur Wikipédia sont diffusés sous licence « Creative Commons paternité partage à l'identique », et peuvent donc être copiés, redistribués, modifiés et même commercialisés à certaines conditions de façon mondiale, perpétuelle et sans redevance[133]. Wikipédia condamne les atteintes au droit d'auteur, tout en reconnaissant que la distinction légale entre *copyright* et *fair use* peut être assez complexe[134].

Questions à vérifier

- *Est-ce que les articles du site Wiki contiennent des œuvres ou parties d'œuvres qui sont protégées par la Loi sur le droit d'auteur ?*
- *Est-ce que le participant détient les autorisations nécessaires pour publier tout ce qui se trouve sur celui-ci ?*

e. La responsabilité pour les informations diffusées

Les sites Wiki sont habituellement dans la position d'un hébergeur et n'ont pas, à ce titre, de responsabilité pour le contenu publié par les participants. Ainsi, s'ils sont avertis qu'un propos illicite se retrouve sur le site, ils ont l'obligation d'effectuer les vérifications appropriées et de le retirer si nécessaire.

La situation se corse, si l'on veut retenir la responsabilité d'un auteur d'un article, puisqu'il y a en général plusieurs auteurs qui y ont coopéré. La personne qui a inséré le propos fautif dans l'article sera responsable. La question de savoir si la dernière personne qui aurait modifié un article même si elle a seulement corrigé certaines fautes

---

133 « Wikipedia : Copyrights », Wikipédia, en ligne : http://en.wikipedia.org/wiki/Wikipedia: Copyrights site consulté le 19 décembre 2011)

134 « Wikipedia : List of Policies », Wikipédia, en ligne : http://en.wikipedia.org/wiki/ Wikipedia_policy#Legal_and_copyright (site consulté le 19 déecembre 2011)

grammaticales est plus délicate. Mais il paraît certain que, si un article comportant un contenu illicite se retrouve sur un site Wiki et que l'auteur est la seule personne qui y a contribué, il en sera responsable.

Question à vérifier :
• *Est-ce qu'il y a un ou plusieurs auteurs à l'article en question ?*

f. L'utilisation des sites wikis à des fins judiciaires

L'information mise en ligne sur Wikipédia n'étant pas constante quant à sa fiabilité, tant les parties que les juges doivent user de discernement quant aux éléments de preuve qui proviennent de cette encyclopédie. Dans certains cas, la preuve provenant de sites Wikis a été considérée acceptable alors que, dans d'autres, elle a été rejetée. Les enquêtes « maison » effectuées sur Google ou Wikipédia par les membres d'un jury afin de « bonifier » la preuve ou de se faire une opinion sur une situation ou sur une personne, témoin ou accusé sont problématiques. Ces pratiques, difficilement contrôlables, affectent nécessairement l'administration de la justice[135].

Dans *R. c. Cianfagna*[136]*,* le tribunal constate que Wikipédia « ne peut pas (encore) être qualifiée d'encyclopédie ». Il ne peut donc être présumé que Wikipédia constitue une source accessible et fiable. Si les caractères d'accessibilité et de fiabilité ne peuvent pas être présumés, ils pourraient par contre être prouvés. Wikipédia constituerait alors une source sur laquelle pourrait se baser un juge pour prendre connaissance d'office d'un fait. Car le tribunal convient que si Wikipédia, dans sa globalité, ne constitue pas une source fiable, certains de ses articles peuvent être fiables.

3. Comment évaluer ces risques ?

L'ampleur du risque auquel on s'expose en naviguant sur des sites Wikis, ou en y participant, varie selon ces facteurs : l'accessibilité au site Wiki, le sujet du site, ainsi que le caractère anonyme ou non des participants.

a. L'accessibilité au site Wiki

Il est certain qu'un site Wiki, disponible seulement au sein d'une entreprise afin que des employés collaborent à un projet, est moins risqué qu'un site se retrouvant sur Internet. En effet, un plus grand contrôle peut être exercé sur un site disponible seulement, par

---

135 John SCHWARTZ, « As Jurors Turn to Web, Mistrials are Popping up », *The New York Times*, 18 mars 2009, en ligne: http://www.nytimes.com/2009/03/18/us/18juries.html (site consulté le 19 décembre 2011).

136 *R. c. Cianfagna*, Cour municipale de Montréal, 2007 CanLII 25904 (QC C.M.), 28 juin 2007, http://www.iijcan.org/fr/qc/qccm/doc/2007/2007canlii25904/2007canlii25904.html.

exemple, sur un intranet, puisque les personnes qui y ont accès sont identifiées et identifiables.

En revanche, un site accessible au grand public et qui peut être modifié par tous les visiteurs risque davantage d'être victime de sabotage par des personnes qui sont mal intentionnées. De plus, cette grande accessibilité fait en sorte que les dommages seront plus grands si, par exemple, des propos diffamatoires y sont publiés.

Question
- *Le site est-il accessible par Internet ou limité à un groupe d'utilisateurs comme un intranet ?*

b. Le contenu du site Wiki

Comme pour les pages Web, certains types de contenus ou d'activités sur un site Wiki sont plus problématiques que d'autres. Les articles portant sur des sujets qui soulèvent des points de vue différents risquent d'être moins impartiaux que des articles dont le contenu est par définition neutre. Par exemple, une personne peut avoir intérêt à prendre le contrôle d'un article qui porte sur une compagnie pour le rendre davantage favorable à l'entreprise. Par contre, il paraît moins probable qu'un individu falsifie un article portant sur des sortes de fleurs ou encore sur les oiseaux puisque le sujet est neutre.

La nature même de l'article peut aussi faire varier les risques. Il peut être risqué d'écrire la biographie d'une personne à son insu puisqu'il est possible que l'on rédige des propos faux ou diffamants. Par contre, un tel risque pourrait se révéler moindre lorsqu'on écrit un article scientifique. Pour certaines entités oeuvrant dans des contextes très concurrentiels, il faut évaluer les dangers de réaliser des tempêtes d'idées, de la recherche et du développement dans le contexte de wikis plus ou moins ouverts.

Questions à vérifier
- *Quel est le sujet de l'article en question ?*
- *Est-ce que la nature de l'article comporte des risques inhérents ?*

c. Le caractère anonyme ou non des participants

Certains sites Wikis autorisent des auteurs anonymes à publier des articles ou des modifications. D'autres exigeront certains renseignements, comme une adresse de courriel valide ou un pseudonyme, afin de publier du contenu. En exigeant certains renseignements permettant d'identifier l'auteur, on diminue les risques étant donné que les participants peuvent craindre de se faire identifier. De plus, certains sites sont plus exigeants en autorisant uniquement les membres à faire des modifications.

Questions à vérifier

- *Est-ce que les participants communiquent dans l'anonymat ?*
- *Est-ce que les participants utilisent des pseudonymes ?*
- *Est-ce qu'il y a des restrictions quant aux personnes pouvant publier un article ?*

4. Quelles sont les précautions à prendre ?

a. Mettre en place une procédure pour répondre aux préoccupations ou plaintes concernant le matériel placé sur le site

Il serait préférable pour un site Wiki de prévoir une procédure simple et efficace pour recevoir les plaintes à l'égard du contenu du site. En effet, une telle méthode est avantageuse autant pour le plaignant que pour les administrateurs du site puisque les recours devant les tribunaux ne sont pas toujours les plus efficaces. La procédure judiciaire peut être longue et coûteuse, et le matériel inapproprié peut rester longtemps sur le site avant qu'un jugement ne soit prononcé. Une procédure à l'interne est donc une bonne alternative. Par exemple, le site peut prévoir que, si une information sur le site semble inappropriée, on puisse déposer une plainte à un groupe de vérification du site qui jugera si le contenu doit être retiré ou non.

b. Établir une politique d'utilisation du site Wiki

Il serait prudent pour un site Wiki de mettre en place une politique d'utilisation des services offerts. Celle-ci préviendrait les gens des usages qui sont acceptés et du contenu qui est prohibé. Par exemple, un site Wiki pourrait prévoir qu'un contenu diffamatoire, à caractère pornographique ou encore menaçant, n'est pas accepté, qu'il est impératif de respecter le droit d'auteur en rédigeant un article... Si ces conditions ne sont pas respectées, le site peut se réserver le droit de supprimer le contenu inapproprié ou encore il pourrait bloquer le compte d'usager d'une personne qui pose des actes malveillants.

La politique d'utilisation du site Wiki devrait également prévoir que les contributeurs au site sont les seuls responsables du contenu qu'ils publient puisque le service offert se limite à héberger de l'information. Un tel avertissement peut être dissuasif pour une personne ayant l'intention de publier un contenu inapproprié. De plus, on peut préciser, si c'est le cas, que les administrateurs du site ne participent aucunement à la création du site. Une telle affirmation, dans le cadre d'un recours judiciaire, peut être utile pour établir la ligne de démarcation entre les personnes responsables et celles qui ne le sont pas.

c. Mettre en place une procédure afin de revoir le matériel placé sur le site Wiki pour vérifier sa conformité au droit d'auteur et à d'autres droits

Certains proposent de mettre en place une procédure pour vérifier les informations qui sont déjà publiées sur le site Wiki, ou qui vont l'être, dans le but de vérifier leur

conformité à la loi. Une telle procédure, même si elle est faite de bonne foi, peut entraîner la responsabilité des administrateurs, si un contenu inapproprié est publié, puisqu'ils ont le contrôle de l'information comme un éditeur.

d. Établir des règles de conduite

Avec l'usage, les collaborateurs aux sites Wikis ont développé certaines règles de conduite que chaque personne doit adopter lorsqu'elle participe à un tel site. Ces conventions peuvent être déroutantes pour un débutant dans le domaine puisqu'elles ne sont pas toujours écrites. C'est pourquoi il est préférable de les consigner par écrit lorsqu'un site Wiki est mis en ligne, afin d'en favoriser leur respect. On peut prévoir, par exemple, la nécessité pour les personnes de réviser le contenu avant de publier un article ou encore de décrire les modifications faites sur la page, dans le but de conserver une trace de ce qui a été fait.

e. Informer les gens des risques inhérents à l'utilisation d'un site Wiki

Il est important de sensibiliser les gens aux risques auxquels ils s'exposent en utilisant les sites Wikis. Les mises en garde peuvent porter sur plusieurs éléments, comme l'obligation de respecter le droit d'auteur ou encore la nécessité de bien se renseigner sur un sujet avant de se fier à une ressource Wiki.

G. Les flux RSS

1. Qu'est-ce qu'un flux RSS ?

Un flux RSS (se dit aussi fil RSS) désigne un format utilisé pour publier du contenu Web régulièrement mis à jour. RSS est l'abréviation de *Real Simple Syndication*. La syndication de contenu (ou agrégation de contenu) consiste à rendre un texte (incluant nom de l'auteur, photo, titre et date) indépendant de la structure du site Web principal. Ainsi, celui qui désire publier un nouveau message n'a pas à mettre à jour sa page Web à chaque entrée. Un site d'actualité utilise les flux RSS pour ses différents sujets (politique, sport, art, etc.). Une entreprise de produits et services utilise le flux RSS pour annoncer ses nouveaux produits. Le flux ressemble à une page Web contenant toutes les nouvelles en ordre chronologique.

Pour l'utilisateur, un agrégateur de contenu (un logiciel comme un navigateur Web ou une application en ligne comme Google Reader) permet de rassembler tous les flux et de les gérer. Pour reprendre notre exemple du site d'actualité, l'utilisateur peut recevoir, dans son agrégateur, les derniers billets de Cyberpresse de la section « Politique ». L'utilisateur n'a plus besoin de naviguer sur les sites pour retrouver ses nouvelles. Les nouvelles viennent à lui. En plus de pouvoir être intégré dans un agrégateur RSS, le flux RSS peut faire l'objet d'incorporation (*embedding*), ce qui signifie que n'importe qui peut ajouter le flux de nouvelles dans son site. Par exemple, le

webmestre d'un site de sport peut intégrer le flux de nouvelles du site d'une équipe sportive à son propre site.

Au plan technique, RSS et Atom sont deux langages informatiques différents permettant la syndication de contenu. Ils se confondent puisque les sites Web utilisent le même logo indépendamment du langage utilisé. Dans tous les cas, le contenu d'un flux RSS est plutôt limité. Il se limite à du contenu texte simple. Toutefois, le standard Atom permet d'ajouter des liens vers des documents photos, audio ou vidéo.

a. Qui fait quoi ?

i) L'utilisateur ou le lecteur

L'utilisateur est la personne physique qui consulte le contenu des flux RSS. Généralement, l'utilisateur gère ses flux par un agrégateur qui lui permet de trier, de classer et de lire un résumé (« chapeau ») des articles d'actualité. Si le chapeau de l'article l'intéresse, l'utilisateur clique sur le lien et est redirigé vers le site Web où l'article est publié en entier. Il est très envisageable que des employés se constituent des pages Web personnelles ou des blogues. Dans ce cas, ils peuvent avoir envie d'y relayer des flux RSS qui sont susceptibles d'intéresser les visiteurs de leur page. Cela dit, il convient de rappeler que n'importe qui peut générer un flux RSS, et que ces flux ne relèvent pas nécessairement du bon goût.

Dans le cadre d'une entreprise ou organisme public, ce peut être un employé qui maintient un fils RSS pour publier son travail récent (exemple : chercheur à l'université).

ii) L'éditeur du contenu

L'éditeur de contenu est la personne qui publie l'article qui sera contenu dans le flux RSS. Les éditeurs de contenus sont multiples. Par exemple, il est possible de s'abonner au flux RSS de Conan O'Brien, un humoriste américain qui publie sur Twitter. À l'opposé, l'Université de Montréal a aussi un fil RSS pour présenter ses plus récents articles. Le flux RSS est donc utilisé par plusieurs sur Internet, et ce, pour des fins bien diverses ; il y existe donc une myriade d'éditeurs de contenus.

iii) Le développeur du site

Le développeur est la personne qui crée, maintient et actualise un site Web. Il arrive de plus en plus que les développeurs utilisent la technique de l'incorporation (*embedding)* pour insérer des flux RSS dans leur propre site ou blogue. Il peut agencer les flux et les répertorier pour les mettre à la disposition de ses visiteurs. De son point de vue, les flux RSS sont des contenus automatisés, car ils se mettent à jour automatiquement. Les sites qui répertorient des contenus automatisés traitant d'un thème commun portent le nom de *mashups* (applications composites).

Lorsque le développeur utilise la technique de l'incorporation (*embedding)*, il relaye le flux RSS. La technique de l'incorporation est très simple et ne requiert pas de connaissance particulièrement poussées pour être intégrée à un site ou à un blogue. Le développeur de site peut être le site d'une entreprise ou d'un organisme, mais aussi, à l'opposé, celui d'un individu.

b. Utilisation des flux RSS

Les flux RSS servent principalement à suivre l'actualité. Pour un travail donné, il est possible de créer un blogue sur lequel s'affichent les flux RSS de sites reliés au sujet. Une entreprise peut utiliser les flux RSS sur son site Web pour relayer, par exemple, des actualités d'un chroniqueur en particulier, les actualités relatives à son domaine d'activités, etc. Elle peut aussi créer son propre flux RSS pour afficher l'actualité de l'entreprise, le calendrier de ses activités, etc.

2. Quels sont les risques associés à un flux RSS ?

La création de son propre flux RSS comporte les mêmes risques que n'importe quelle publication sur Internet. À l'instar des autres applications supposant la diffusion d'informations comme le blogue, la page Web personnelle, l'espace personnel sur un réseau social, l'éditeur du contenu est responsable des propos qu'il diffuse. Mais le flux RSS comporte un risque particulier : celui qui découle de l'utilisation d'un flux publié par un tiers.

a. Engager sa responsabilité pour le contenu du flux RSS publié par un tiers

Un webmestre qui n'est pas l'auteur d'un document litigieux relayé par un fil RSS mais qui fait le choix de le publier à l'intérieur d'un agencement particulier sur son site pourrait avoir à répondre du contenu qui se trouverait ainsi diffusé même s'il est généré automatiquement. Il en irait ainsi également s'il connaît le caractère illicite des messages qu'il relaie par le truchement d'un fil RSS rendu disponible sur son site.

Une entreprise peut relayer les flux RSS de ses employés. Les employés peuvent générer des flux RSS via leurs pages Twitter/MySpace ou leurs blogues. Si un employé rédige des propos médisants au sujet d'une autre personne, ses propos seront alors disponibles à un bien plus grand lectorat. L'entreprise ou l'organisme risque alors d'être tenu responsable envers la personne victime des propos médisants.

Dans l'hypothèse où l'entreprise ou l'organisme génère son propre flux RSS, elle doit agir avec diligence, au même titre que tout autre contenu publié sur sa page Web.

Questions à vérifier :
- *Les flux des tiers relayés sur le site de l'entreprise ou de l'employé sont-ils entretenus par des gens de confiance?*
- *Le site Web de l'entreprise ou de l'organisme public est-il surveillé afin de réagir rapidement?*

3. Comment évaluer ces risques ?

a. Le sujet du fils RSS

Le sujet du fils RSS a une incidence dans le risque. Si le fils RSS qui est relayé est un blogue où l'auteur se permet des nouvelles plus personnelles – donc un fils RSS avec un sujet large – il est plus risqué de dévoiler de l'information personnelle hors contexte que pour un blogue à sujet plus impersonnel.

b. Le public cible du site propulsé par le développeur

Un site qui s'adresse à un large public comporte nécessairement plus de risques qu'un site lu par seulement quelques personnes. À qui s'adresse le site ? Le public cible joue un rôle important. Il suffit de prendre pour exemple le site d'une entreprise destiné aux clients et aux membres du personnel. Un propos médisant n'aura certainement pas le même impact que s'il était seulement publié sur la page Twitter/Facebook destinée aux quelques amis d'un individu.

c. La place et l'importance attribuées au flux RSS

L'accent mis sur le flux RSS peut jouer un rôle dans la détermination de la fonction éditoriale et dans la connaissance du développeur de pratiques illicites. Dans un premier cas de figure, le flux RSS est disponible sur la page d'accueil du site, et le site est construit autour de ce flux RSS. Dans un deuxième cas de figure, le flux RSS se situe dans une section discrète intitulée « Partenaires ». Il y a beaucoup plus de risques que, dans le premier cas, on assimile le développeur du site à un éditeur. Dans le deuxième cas, le développeur risque moins d'être assimilé à un éditeur mais peut tout de même se faire imputer une connaissance de la teneur illicite de certains contenus.

4. Quelles sont les précautions à prendre ?

a. Vérifier le site régulièrement

L'une des façons pour le développeur d'éviter d'engager sa responsabilité est de retirer promptement le contenu dès qu'il a connaissance de son caractère illicite. Pour ce faire, le développeur peut visiter régulièrement son site et prendre connaissance des titres, chapeaux et images qui sont relayés via les flux RSS. Dès qu'un contenu possiblement illicite apparaît, le développeur peut se désabonner du flux RSS. Ainsi, il minimise ses risques de partager la responsabilité avec l'éditeur du contenu.

b. Ne relayer que des sites crédibles

Il existe sur Internet une abondance de flux RSS. Lorsque vient le temps de créer une page Web ou un site institutionnel, il convient de ne relayer que des sites dont on peut attester de la crédibilité.

H. La baladodiffusion

1. Qu'est-ce que la baladodiffusion ?

Le mot « podcast » résulte de la combinaison des mots « iPod » (le lecteur MP3 d'Apple) et « broadcast »[137]. Ce type de fichier est appelé « balado »[138] selon l'Office québécois de la langue française.

Les balados sont des dossiers médias numériques qui peuvent être téléchargés sur ordinateur et qui peuvent être transférés sur un lecteur multimédia portatif. Les gens accèdent aux balados de plusieurs façons : via un lien RSS (*Really Simple Syndication*) qui peut être accessible depuis la plupart des navigateurs Internet et par le biais du magasin en ligne iTunes, ou alors via d'autres programmes mettant en ligne des balados.

Malgré les origines de son nom, il n'est pas nécessaire de posséder un iPod ou un MP3 pour écouter un balado. Il est en effet possible de télécharger le fichier balado directement du navigateur ou alors il est possible de s'abonner à un balado[139].

Le modèle de syndication RSS permet à l'usager de recevoir des mises à jour automatiques quand de nouveaux balados sont disponibles pour le téléchargement. Une fois entrés les paramètres préférés de l'utilisateur quant aux balados, ceux-ci seront automatiquement téléchargés sur son ordinateur[140]. Par exemple, un utilisateur possédant iTunes (le logiciel de musique d'Apple) se rend sur le *iTunes Store* où des centaines de balados sont à sa disposition. Il pourra alors choisir ceux qu'il souhaite télécharger dans son ordinateur. Il peut aussi décider de s'abonner – gratuitement ou non – aux balados qu'il aime et ces derniers seront automatiquement téléchargés sur son ordinateur à chaque fois qu'une nouvelle mise à jour (ou épisode) sera disponible.

---

137 Kathleen Elliott VINSON, « What's on Your Playlist ? The Power of Podcasts as a Pedagogical Tool » (2009), 09 *Legal Studies Research Paper Series*, en ligne: http://ssrn.com/abstract=1337737 (site consulté le 19 décembre 2011).

138 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Balado », 2006, en ligne : http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/dictionnaires/internet/fiches/8357110.html (site consulté le 19 décembre 2011).

139 Kathleen Elliott VINSON, « What's on Your Playlist? The Power of Podcasts as a Pedagogical Tool », (2009), *Legal Studies Research Paper Series*, en ligne : http://ssrn.com/abstract=1337737 (site consulté le 19 décembre 2011).

140 Erin M. JACOBSON, « Podcasting 201 : Copyright Infringement Issues when Using Third-party Material in Podcasts », (2008) 26-1 *The Entertainment and Sports Lawyer* 7.

L'hôte ou l'auteur du fichier balado est appelé baladodiffuseur[141]. La création de balados est simple; cela ne demande pas la technologie d'un studio d'enregistrement professionnel. En effet, un microphone ou un téléphone cellulaire équipé des programmes nécessaires permettent tous deux l'enregistrement de balados. Même si, au départ, la baladodiffusion a été créée pour diffuser du contenu audio sur Internet, la technologie permet aussi d'avoir accès à des fichiers sous forme de vidéos[142].

Un balado peut avoir une durée variant de quelques secondes à plusieurs heures. Certains des balados sont gratuits, alors que d'autres ne sont disponibles que moyennant le paiement d'un abonnement.

a. Qui fait quoi ?

i) L'agrégateur

Les balados peuvent être automatiquement téléchargés selon les préférences de l'usager au moyen d'un logiciel d'agrégation – appelé agrégrateur, ou tout autre service de distribution Internet comme le protocole RSS (*Really Simple Syndication*) . En fait, un agrégateur (de l'anglais *aggregator*) est un logiciel qui permet de suivre plusieurs fils de syndication (RSS) simultanément[143]. Par extension, l'entité qui a la maîtrise du logiciel d'agrégation à l'égard d'un ensemble de balados est l'agrégateur.

L'utilisateur n'a donc pas besoin de visiter tous les sites pour savoir s'il y a eu changement au niveau des fichiers balados disponibles puisqu'il obtient l'information automatiquement.

ii) L'hébergeur/l'éditeur

L'éditeur est l'entité qui exerce un contrôle effectif sur la sélection des contenus de même que sur leur organisation, soit sur une grille chronologique, dans les cas d'émissions télévisées, soit sur un catalogue, dans le cas de services de médias audiovisuels à la demande. Le balado que l'éditeur met en ligne peut être sa création ou celle d'un tiers mais il sera, dans les deux cas, responsable du contenu.

---

141 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Baladodiffuseur », 2006, en ligne : http://www.granddictionnaire.com/BTML/FRA/r_Motclef/index800_1.asp (site consulté le 19 décembre 2011).

142 Holly Beth BILLINGTON, « The Podcasting Explosion : US and International Law Implications », (2006) 18-11 *Intel. Prop. & Tech. L. J.* 5

143 Wikibena, « Baladodiffusion », en ligne : https://wiki.umontreal.ca/display/BENA/Utiliser+la+baladodiffusion#Utiliserlabaladodiffusion7.4%C3%89tapeIVRendrevotrebaladoreconnaissableentre tous (site consulté le 19 décembre 2011).

L'auteur du balado, qu'on appelle « *podcaster* » en anglais, se nomme baladodiffuseur ou baladiffuseur en français[144]. Il crée le fichier balado pour le rendre disponible en ligne. Il est le diffuseur, « qui, par l'entremise d'un abonnement à des fils de syndication, diffuse sur Internet des balados audio ou vidéo, téléchargés automatiquement à l'aide d'un logiciel agrégateur et destinés à être transféré sur un baladeur numérique ou sur un ordinateur pour une écoute ou un visionnement ultérieurs ».

Si un site ne fait qu'héberger le contenu des balados et ne participe pas à leur création ou à la décision de diffuser, alors il sera, selon toute probabilité, considéré comme étant un hébergeur.

iii) Utilisateur

L'utilisateur est l'acteur central de la baladodiffusion. En effet, le fichier balado est créé pour que celui-ci puisse l'écouter. Lorsque l'utilisateur identifie un balado intéressant, il a trois possibilités : il peut en faire une lecture en transit (en *streaming*) sans télécharger le fichier, il peut télécharger le fichier balado sans aucune application – ce qui peut être possible sur certains sites – ou, finalement, il peut le télécharger par le biais d'une application telle *Juice, iTunes, Netvibes*, puis le transférer sur son baladeur[145].

L'utilisateur peut également choisir de s'abonner aux fichiers balados qui l'intéressent. Il recevra alors automatiquement dans son agrégateur chaque mise à jour du fichier balado qui l'intéresse. L'usager pourra alors les écouter sur son ordinateur ou son lecteur MP3[146].

L'auteur des balados met les fichiers en ligne et c'est alors « aux auditeurs que revient le rôle de gérer une liste de lecture avec leurs différents abonnements. Le téléchargement des fichiers est alors automatisé et issu des multiples sources qu'ils ont choisies. En d'autres termes, c'est l'auditoire qui choisit des baladodiffuseurs et les mises à jour des nouveaux balados seront automatiques dans leur agrégateur »[147].

---

144 OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, « Baladodiffuseur », (2006), en ligne : http://www.granddictionnaire.com/BTML/FRA/r_Motclef/index800_1.asp (site consulté le 19 décembre 2011)

145 Anne-Sophie JOUANNON, « Les enjeux juridiques du podcasting », (2008) *Mémoire de master Université de Versailles, St-Quentin-en-Yvelines*.

146 Anne-Sophie JOUANNON, « Les enjeux juridiques du podcasting », (2008) *Mémoire de master Université de Versailles, St-Quentin-en-Yvelines*.

147 Wikibena, « Baladodiffusion », en ligne : https://wiki.umontreal.ca/display/BENA/Utiliser+la+baladodiffusion#Utiliserlabaladodiffusion7.4%C3%89tapeIVRendrevotrebaladoreconnaissableentretous.

b. Utilisation de la baladodiffusion

L'objectif initial de la baladodiffusion était de rendre disponible les programmes de type radios, et cela demeure, à ce jour, l'usage le plus répandu[148]. Le contenu des balados peut se composer d'informations comme celles émanant de blogues audio privés. Il peut être constitué de fichiers audio ou vidéo d'émissions déjà diffusées. On y retrouve aussi de la programmation originale créée spécialement pour la diffusion en ligne[149] comme des conférences, des horoscopes ou des radios indépendantes diffusant sous forme de balados.

Par exemple, un marché important s'est développé au sein de l'industrie du voyage et du tourisme. Ainsi, plusieurs hôtels offrent dorénavant la possibilité d'utiliser les lecteurs audio portatifs pour se promener dans une ville donnée au lieu des guides de voyage traditionnels. Les balados sont également utilisés en politique. Le département d'État publiait, sous forme de balado, les discours de la secrétaire d'État Condoleezza Rice. Le service de police de la ville de New York rend disponible, en baladodiffusion, des conseils de sécurité ainsi que des communiqués de presse[150]. Autre exemple, la radio de Radio-Canada offre des émissions en ligne gratuitement en baladodiffusion. La plupart des sites de baladodiffusion disponibles au Québec sont accessibles sur le site http://quebecbalado.com/. Des entreprises utilisent ce type de véhicule pour offrir des tutoriels (exemple : pour l'utilisation d'un logiciel).

2. Quels sont les risques associés à la baladodiffusion ?

Les risques des balados sont les mêmes que pour les autres environnements de diffusion et de partage de contenus dans les réseaux (l'utilisation non autorisée de l'image et de renseignements personnels, les atteintes au droit d'auteur, la présence de contenu illicite, les contenus haineux, menaçants, diffamatoires et contraires aux lois).

3. Comment évaluer ces risques ?

Pour évaluer les risques spécifiques à la diffusion et au partage de contenus au moyen de balados, il est opportun de s'interroger sur le public visé, la présence de sons, d'images ou de vidéos, ainsi que les types d'informations concernées.

---

148 Gavin SUTTER et Johanna GIBSON, « Podcasts and the Law », (2007) *JISC legal information*.

149 Holly Beth BILLINGTON, « The Podcasting Explosion : US and International Law Implications », (2006) 18-11 *Intel. Prop. & Tech. L. J.* 5

150 Holly Beth BILLINGTON, « The Podcasting Explosion: US and International Law Implications », (2006) 18-11 *Intel. Prop. & Tech. L. J.* 5

a. Le public visé

Le public cible visé peut moduler les attentes qu'une personne peut avoir en écoutant un balado. Ainsi, le contenu d'un fichier balado diffusé pour des enfants devra être approprié en fonction de leur âge. De plus, la diffusion d'un balado sur l'intranet d'une institution ne présente pas les mêmes risques que la diffusion du même fichier sur le Web en général. Les informations qui y seront consignées devront tenir compte du public auquel il est adressé.

> ***Question à vérifier***
> *Quelles personnes auront accès au balado ?*

b. La présence de sons, d'images ou de vidéos

La présence de matériel protégé par le droit d'auteur dans un balado augmente les risques pour un créateur. En effet, bien que le fichier balado soit une nouvelle création, la présence de tout matériel protégé ou sous licence peut engager la responsabilité de l'auteur qui a utilisé le matériel sans obtenir les autorisations nécessaires.

> ***Questions à vérifier***
> - *Retrouve-t-on du contenu sous droit d'auteur dans le balado ?*
> - *Si oui, a-t-on obtenu les autorisations nécessaires pour les utiliser dans le balado ?*
> - *Y-a-t-il un mécanisme de licence mis en place et protégeant le fichier balado ?*

c. L'information contenue dans le fichier balado

Les fichiers balados peuvent traiter d'une multitude de sujets. Certains sont enregistrés dans des studios d'enregistrement de radios nationales, alors que d'autres sont créés à même des téléphones cellulaires de particuliers. L'accès à ces fichiers se fait de différentes façons, selon qu'on souhaite télécharger le balado sur un lecteur MP3 ou sur un ordinateur personnel, ou qu'on ne souhaite l'écouter qu'en lecture en transit.

De plus, les fichiers balados ne sont pas toujours accessibles à tous, et ne sont parfois diffusés que sur l'intranet d'une organisation. Dans d'autres cas, les baladodiffuseurs visent un large public et mettent en ligne des sujets aussi variés qu'une émission satirique de l'actualité, un bulletin de nouvelles, une chronique arts et beauté… Les sujets varient, et les registres de langage dans lesquels ils sont faits varient également. La qualité des informations qu'on trouve dans les balados varie tout autant que la forme sous laquelle on peut trouver ledit fichier. Il est facile, pour une personne, de créer son balado et d'y mettre tout le contenu qu'elle décide. Il faut donc faire preuve d'esprit critique et analyser la validité de l'information qu'on reçoit.

4. Quelles sont les précautions à prendre ?

a. Prévoir un moyen de dénoncer le contenu inapproprié

Bien que la dénonciation de contenu inapproprié ne soit pas le moyen le plus utilisé en matière de baladodiffusion, il pourrait être utile pour un site agrégateur – comme iTunes par exemple – de prévoir un moyen de signaler les atteintes aux droits ou la présence de contenu inapproprié dans un fichier balado.

L'entreprise peut, si elle met son podcast sur son propre site, mettre en place un mécanisme pour signaler les atteintes, ou peut-être laisser une adresse courriel à contacter pour le faire.

b. Éviter de porter atteinte aux droits d'autres personnes

Il vaut toujours mieux demander la permission écrite des personnes créatrices des œuvres afin d'utiliser leur voix ou leur image dans un balado. On s'assure ainsi de ne pas attenter aux droits de tiers et l'on protège l'intégrité intellectuelle de notre œuvre. Si l'on souhaite utiliser une partie ou la totalité de l'œuvre d'une autre personne (comme une œuvre musicale), la règle générale veut que, l'on doive obtenir la permission de la personne qui en détient les droits. Et cela est vrai, que l'œuvre soit écrite, filmée ou musicale[151].

Dans le cas où l'obtention de permissions se révèle impossible, il peut être intéressant de vérifier si l'œuvre est protégée par une licence permettant l'utilisation partielle du matériel – comme la licence *Creative Commons*. Dans l'affirmative, il est important de regarder la catégorie de licences qui a été choisie et, dans le cas où une protection minimale a été choisie par l'auteur, il pourrait être possible d'utiliser l'œuvre. Cela n'est toutefois pas une tendance générale pour l'ensemble des créations auxquelles on a accès, et il est important d'assurer une vérification de chacun des fichiers que l'on souhaite utiliser. Sinon, le baladodiffuseur portera atteinte aux droits de tiers et pourra voir sa responsabilité engagée.

151 Gavin SUTTER et Johanna GIBSON, « Podcasts and the law », 11 avril 2007, *JISC Legal Information.*

IV. Les modèles de politiques, de mises en garde et de conseils

MISE EN GARDE

Les modèles de politiques, de mises en garde et de conseils ne sont présentés qu'à titre d'exemple et ne sont pas conçus pour être utilisés tels quels. Comme nous l'avons vu tout au long de ce guide, les enjeux et les risques sont différents d'un site Web 2.0 à un autre. Les politiques doivent alors prendre en considération ces différences, ainsi que les caractéristiques de l'organisation concernée ou du site Internet visé.

A. Politiques générales relatives à l'utilisation d'Internet

1. Politique d'utilisation du site Internet

Il est préférable, pour chaque site Internet, de mettre en place une politique d'utilisation spécifique pour informer les utilisateurs des conduites qui sont tolérées ou non sur celui-ci. Voici un exemple de politique d'utilisation d'un blogue, qui peut être facilement adapté selon le type de site Web 2.0 visé :

> ***Expliquer le fonctionnement et les risques liés à l'utilisation des blogues***
>
> ***Exemple*** *: Le blogue permet à une personne de créer facilement une page Web qui peut porter sur une diversité de sujet. Il se présente sous la forme de billets ou articles publiés sur le site, du plus récent jusqu'au plus ancien. Il est facile à mettre à jour et les visiteurs du site ont habituellement la possibilité de commenter les billets.*
>
> *Le blogue est accessible à un grand nombre de gens. Il faut donc porter une attention particulière au contenu que l'on publie. Le blogueur sera tenu responsable du contenu qu'il publie sur son blogue, il peut être reconnu comme preuve valable pour établir un fait ou un acte juridique.*
>
> *Le blogue peut donner lieu à la transmission d'information causant des préjudices à des personnes. Par imprudence, on peut révéler des éléments de la vie privée d'une personne, des propos peuvent porter atteinte à la réputation, des fichiers peuvent comporter l'usage non autorisé de l'image d'une personne. L'outil peut parfois être utilisé pour la harceler ou menacer.*
>
> ***Préciser les usages autorisés et les utilisations prohibées***
>
> ***Exemple*** *: Le service d'hébergement de blogues doit être utilisé uniquement pour les fins suivantes : (--------décrire les finalités acceptées ou tolérées, par exemple, créer et administrer un blogue portant sur des sujets conformes avec la loi en vigueur-----------).*
>
> *Il faut éviter de révéler des informations sur des tiers, en particulier, il faut être prudent lorsqu'on publie un billet concernant des événements de notre vie privée. Il est toujours prudent de réviser un billet ou un commentaire avant de le publier.*
>
> *Il est interdit de transmettre du matériel haineux, pornographique ou harcelant ou à l'égard duquel on ne détient pas les droits d'auteur.*

Rappeler que l'utilisateur peut être tenu responsable des propos publiés sur son blogue

***Exemple** : Sur Internet, l'utilisateur est doté d'une grande maîtrise de ce qui lui est transmis ou de ce qu'il transmet. Personne n'est en mesure de l'empêcher de recevoir ou de diffuser de l'information s'il a vraiment envie de recevoir ou diffuser. En revanche, l'individu est le premier responsable de ce qu'il reçoit ou de ce qu'il transmet sur Internet.*

En dépit de la grande liberté que le réseau Internet laisse aux personnes, il existe dans tous les pays des lois délimitant ce qui peut ou non être transmis, reçu ou possédé par les personnes. Chaque utilisateur a l'obligation de respecter ces lois. Sinon, de lourdes sanctions peuvent lui être imposées.

Rappeler les principes de respect des droits des personnes

Le droit à la vie privée

***Exemple** : Toute personne a droit au respect de sa vie privée. Il est ainsi interdit de porter atteinte à la vie privée d'une personne.*

Par exemple, on ne doit pas révéler des éléments de l'intimité d'une personne comme sa vie personnelle et familiale (exemple : vie sentimentale ou sexuelle, son état de santé, sa vie familiale, son domicile, ses opinions politiques, religieuses ou philosophiques, son orientation sexuelle, son anatomie, son intimité corporelle...)

Le droit à la réputation des personnes

***Exemple** : Toute personne a droit au respect de sa réputation. Il est ainsi interdit de porter atteinte à la réputation d'une personne, en l'exposant à la haine ou au mépris et en lui faisant perdre l'estime ou la confiance des autres à son égard.*

Par exemple, affirmer ou insinuer des faits sur une personne d'une façon négligente ou téméraire, sans avoir d'abord vérifié la véracité des propos. Ou encore, s'agissant de faits véridiques, les rappeler sans motif légitime dans le seul but de nuire, ridiculiser, humilier, injurier ou insulter une personne.

Le droit à l'image des personnes

***Exemple** : Il est interdit de capter ou de diffuser l'image ou la voix d'une personne lorsqu'elle se trouve dans un lieu privé sans son consentement. Lorsque la personne se trouve dans un lieu public, il est conseillé fortement d'obtenir son consentement à la diffusion, surtout s'il est possible de l'identifier.*

Par exemple, envoyer, via une liste de diffusion, une photo d'une personne sans son autorisation, diffuser la photo d'une personne sur un site Web ou un blogue sans son autorisation, diffuser sur Internet une vidéoconférence sans l'autorisation des participants...

Expliquer comment le droit d'auteur s'applique aux informations trouvées sur l'Internet

***Exemple** : La plupart des textes, images, dessins, sons, œuvres musicales que l'on trouve sur Internet sont protégés par le droit d'auteur.*

Le droit d'auteur est le droit exclusif de décider de diffuser, de reproduire ou autrement communiquer une œuvre au public, de la publier, de l'adapter, de la traduire.

Sauf lorsque cela est explicitement mentionné, on ne doit jamais prendre pour acquis que l'on peut copier, reproduire et diffuser quelque contenu que ce soit qui se trouve sur Internet. Il faut, en général, demander l'autorisation pour reproduire et diffuser une œuvre, par exemple, sur une page Web ou dans une liste publique de discussion.

Rappeler les principes de respect des lois d'ordre public

Il s'agit ici d'expliquer que des lois existent afin de prévenir des conflits ou des comportements qui sont considérés comme contraires aux valeurs de notre société. Il en est ainsi pour les informations à caractère pornographique, la propagande raciste et l'incitation à la haine.

Propagande haineuse

***Exemple** : Il est interdit de tenir des propos qui constituent de la propagande haineuse. La propagande est une action exercée sur l'opinion pour l'amener à adopter certaines idées politiques, sociales ou autres; elle sera dite haineuse lorsqu'elle vise à créer une aversion profonde contre certains groupes de personnes.*

Par exemple, préconiser l'extermination des membres d'un groupe à cause de leur couleur, de leur race, de leur religion, de leur origine ethnique ou de leur orientation sexuelle; communiquer publiquement des déclarations (par des mots, parlés, écrits ou enregistrés, des gestes ou des signes) qui incitent à la haine contre un groupe se différenciant par sa couleur, sa race, sa religion, son origine ethnique ou son orientation sexuelle et qui sont susceptibles d'entraîner une violation de la paix; communiquer des propos, autrement que dans une conversation privée, qui encouragent ou essaient de convaincre les gens de haïr un groupe identifiable par la couleur, la race, la religion, l'origine ethnique ou l'orientation sexuelle.

La propagande haineuse diffère des propos exprimant des opinions légitimes à l'égard de groupes, de religions ou d'entités.

Matériel obscène

***Exemple** : Le matériel obscène, c'est-à-dire le matériel qui exploite les choses sexuelles de façon dégradante ou déshumanisante, n'est pas toléré dans notre société. Ce matériel doit être proscrit, et ce, même en l'absence de cruauté et de violence.*

Pornographie juvénile

***Exemple** : La pornographie juvénile s'entend de représentations graphiques, photographiques, filmées, vidéos ou autres, réalisées ou non par des moyens mécaniques ou électroniques de mineurs se livrant à des activités explicitement sexuelles.*

L'utilisation d'Internet pour communiquer avec un enfant dans le but de commettre une infraction sexuelle contre cet enfant ainsi que de transmettre, de rendre accessible, d'exporter de la pornographie juvénile ou d'y accéder constituent des infractions. La loi permet aux tribunaux d'ordonner la suppression de la pornographie juvénile affichée sur

un ordinateur canadien et permet la confiscation de matériels ou d'équipements utilisés pour commettre une infraction.

Préciser les conséquences d'un comportement indésirable

***Exemple** : Le site d'hébergement de blogues se réserve le droit de fermer un blogue qui serait contraire à la présente politique ou de bloquer le compte d'une personne ne s'y conformant pas.*

2. Politique de protection de la vie privée

Voici un exemple de politique de protection de la vie privée compatible avec la *Loi sur la protection des renseignements personnels dans le secteur privé*[152], qu'il est possible d'intégrer à un site Web 2.0 :

Objet

Nous sommes particulièrement attentifs à préserver la confidentialité des données des usagers qui utilisent ce site. Ainsi, aucune donnée nominative n'est présente sur ce site. Par ailleurs, dans la conduite de nos opérations, nous nous efforçons de respecter en tout temps la confidentialité de vos données personnelles et ce, en accord avec la politique de protection de la vie privée qui suit.

Information recueillie lors de la fréquentation du site

- *Information obtenue lors de l'inscription*

Lors de l'inscription, certaines données seront requises pour pouvoir s'abonner au site Internet. Elles ne seront en aucun cas divulguées à un tiers.

- *Information obtenue lors de votre accès au site*

Comme pour tout site Web, les serveurs qui hébergent nos sites identifient l'adresse Internet (IP) de votre connexion Internet afin de permettre l'échange de données entre nos serveurs et votre ordinateur. Aucune information permettant de vous identifier n'est associée à votre adresse IP.

- *Informations obtenues par les «fichiers-témoins» (cookies)*

Les «cookies» ou fichiers témoins sont de petits fichiers texte qui sont téléchargés sur votre disque dur lorsque vous visitez certaines pages Web. Ces fichiers sont inoffensifs pour votre ordinateur sur lequel vous avez le plein contrôle. Nos serveurs utilisent ces témoins afin de personnaliser l'affichage des pages et afin de recueillir certaines statistiques d'utilisation de nos sites. Il vous est cependant possible en tout temps de modifier la configuration de votre ordinateur ou de votre logiciel fureteur et de ne plus accepter le téléchargement des cookies.

---

152 L.R.Q., c. P-39.1

Finalité de la collecte d'information

L'information obtenue lors de l'inscription au site Internet n'est nécessaire que pour avoir accès aux différentes sections du site. L'information concernant l'adresse IP n'est utilisée que pour permettre l'échange de données entre nos serveurs et votre ordinateur. L'information obtenue par les fichiers-témoins est utilisée pour personnaliser l'affichage des pages Internet.

Communication de l'information

Les données recueillies par le site Internet ne seront en aucune façon communiquées à des tiers, que ce soit dans le cadre d'une liste de diffusion ou dans le cadre d'un concours promotionnel. Elles pourront toutefois être divulguées lorsque la loi nous en oblige.

Détention et sécurité des données

Les données recueillies seront conservées sur les serveurs du site Internet pour la période nécessaire à la réalisation des finalités mentionnées. Ces données seront protégées et les employés n'y auront pas accès.

Accès à votre dossier

Vous pouvez en tout temps consulter ou rectifier les données vous concernant en nous contactant par courrier électronique à l'adresse suivante : (inscrire l'adresse de courrier électronique).

3. Politique de gestion du droit d'auteur et des autres propriétés intellectuelles

Voici un exemple de politique de gestion du droit d'auteur et des autres propriétés intellectuelles :

La propriété intellectuelle fait référence à la protection des droits d'un auteur sur une œuvre qu'il a créée, écrite ou exprimée. La propriété intellectuelle inclut la protection du droit d'auteur, des marques de commerce ainsi que des inventions. Dans la poussée actuelle du développement des nouvelles technologies de l'information, où la reproduction éphémère et l'enregistrement digital sont la norme, le concept de la propriété intellectuelle est devenu fondamental. Internet, le courriel et les pages Web fournissent de multiples forums permettant la création de graphiques, de textes, d'œuvres d'art et de musique, en plus des multiples opportunités pour les tiers de se les approprier. Certaines solutions techniques s'offrent à l'utilisateur désireux de protéger ses œuvres.

Il convient toutefois d'avoir toujours à l'esprit que :

- *Les images, textes et créations trouvées sur Internet sont la propriété de leur créateur. Tout usage de telles œuvres nécessite l'autorisation de leur auteur.*

> - *L'utilisation, la publication et la retransmission de la musique, des images, des textes, des pages Web et autres informations trouvées sur Internet sont soumises aux restrictions énoncées dans la loi sur le droit d'auteur.*
> - *Le piratage de logiciel informatique, la reproduction sur CD-Rom ou par retransmission sont des actes interdits par la loi.*
>
> *Le contenu publié sur le site Internet et qui est en contravention avec les lois sur le droit d'auteur sera retiré du site, et ce, sans aucun préavis.*

B. Politiques et précautions spécifiques selon le type de site Web 2.0 utilisé

1. Les blogues

Pour rendre plus agréable la navigation sur les blogues, il convient d'adopter une nétiquette qui mentionne les comportements qui ne sont pas tolérables sur le blogue, ainsi que les règles de savoir-vivre[153]. Elle s'applique autant aux blogueurs qu'à ceux qui publient des commentaires. Ces règles ont été établies, avec l'usage, par les blogueurs, et en voici des exemples :

- *Ne pas employer un langage vulgaire, menaçant, diffamant, insultant ou faire des commentaires racistes, à connotation ethnique ou contraire à la loi.*
- *Les commentaires à caractère pornographique et la publicité ne sont pas acceptés.*
- *Respecter, en tout temps, le droit d'auteur, et mentionner la source exacte lorsque des citations ou des extraits d'une œuvre sont employés.*
- *Éviter les mots écrits en majuscule, cela donne l'impression de crier.*
- *Ne pas publier de commentaires anonymes. L'utilisation d'un pseudonyme est acceptée, mais il faut fournir une adresse de courriel valide.*
- *Pour résoudre un conflit qui s'amplifie, il faut essayer de le faire en privé avant de publier des commentaires.*

---

153 Pour voir des exemples de nétiquettes qui ont été adoptées : LES HUMAINS ASSOCIÉS, *Une nethique pour le blog 1.0*, http://nethique.info/charte; Éric DELACROIX, *Une nétiquette pour les blogs*, http://www.ed-productions.com/leszed/index.php ?2005/10/27/179-une-netiquette-pour-les-blogs; Mario TOUT DE GO, *Politique éditoriale de « Mario, tout de go »*, http://carnets.opossum.ca/mario/archives/2003/07/politique_edito.html; Tom O'REILLY, *Draft Blogger's Code of Conduct*, http://radar.oreilly.com/archives/2007/04/draft_bloggers_1.html; BLOGHER, *What are your community guidelines ?*, http://www.blogher.com/what-are-your-community-guidelines

Pour une version Wiki de la nétiquette en français, voir le site Blogging Wikia : *Code de conduite pour la blogosphère par Tim O'Reilly*, http://blogging.wikia.com/wiki/Code_of_conduct_in_French.

2. Les sites de partage de contenu

Pour les sites de partage de contenu, il peut être nécessaire de reprendre la politique de gestion du droit d'auteur et des autres propriétés intellectuelles et de la mettre plus en évidence sur le site Internet. En effet, la violation du droit d'auteur est un des risques les plus importants sur les sites de partage de contenu.

3. Les sites de réseaux sociaux[154]

Pour minimiser les risques que représentent les sites de réseautage social, il peut être important de mettre en ligne des conseils de sécurité[155].

- Ne pas oublier que le site de réseautage social est un endroit public. Par conséquent, il est prudent de ne pas révéler une information que nous ne voudrions pas que tout le monde connaisse.
- Il faut éviter de révéler des informations personnelles nous concernant. Des renseignements tels notre adresse, notre nom complet, notre numéro de téléphone, notre date de naissance ou encore notre numéro d'assurance sociale ne devrait pas être communiqués.
- De la même façon, nous ne devrions pas publier des informations que nous ne voudrions pas dévoiler à notre employeur ou encore à nos parents. En effet, ceux-ci peuvent parfois naviguer sur le site et voir ces renseignements. Si nous ne voulons pas qu'ils les voient, c'est un indice que nous ne devrions peut-être pas publier le contenu en question.
- Il est prudent d'accepter seulement sur notre liste de contact les gens que nous connaissons bien. En effet, cela évite qu'un profil, mis à la disposition des amis exclusivement, puisse être vu par des inconnus.
- Les usagers des sites de réseautage social ne sont pas toujours les gens qu'ils prétendent être. Il faut donc être prudent avant de dévoiler à quelqu'un des éléments de notre vie privée ou de faire des confidences. De plus, nous ne devrions pas rencontrer des personnes inconnues. Dans le cas contraire, le rendez-vous devrait être pris dans un endroit public et en présence d'une personne de confiance, comme un parent.

---

154 Pour une méthode complète décrivant les demarches à faire afin d'établir une politique sur les médias sociaux dans les entreprises, voir: Didier DUBOIS, Emilie PELLETIER et Katherine POIRIER, *Comment bâtir votre politique d'utilisation des médias sociaux*, Cowanville, Éditions Yvon Blais, 2011.

155 Pour voir des exemples de conseils de sécurité qui ont été adoptés : MYSPACE, *MySpace Safety Tips*, http://www.myspace.com/help/safety/tips WIRED SAFETY, *Parry Aftab's Guide to Keeping* http://internetsafetyeducator.com/internet-safety-downloads/socialnetworktips.pdf; WINDOWS LIVE SPACES, *Sécurité*, http://spaces.live.com/default.aspx ? page=Ed05&ss=False

- Si nous sommes mal à l'aise face au comportement d'un usager, que ce soit parce qu'il propage des menaces, qu'il met en ligne des photographies, de nous ou qu'il incite à des actes sexuels, il ne faut pas hésiter à le dénoncer.
- Les messages non sollicités, à connotation sexuelle, devraient être complètement ignorés. Ces propos devraient par contre être rapportés aux administrateurs du site ou à une personne de confiance.

4. Les sites d'évaluation de personnes, de services ou de produits

Pour rendre plus agréable la navigation sur les sites d'évaluation de personnes, de produits ou de services, il convient d'adopter des règles concernant l'écriture des commentaires sur le site[156]. Ces règles mentionnent les types de propos qui sont tolérés ou non sur le site, dans le but d'éviter, entre autres, que des commentaires déplacés ou illicites soient publiés. Ces règles ont été établies, avec l'usage, par les utilisateurs, et en voici des exemples :

> - *Il faut laisser des évaluations et des commentaires utiles.*
> - *Ne pas employer un langage vulgaire, menaçant, diffamant, insultant ou faire des commentaires racistes, à connotation ethnique ou contraire à la loi.*
> - *Les commentaires à caractère pornographique et la publicité ne sont pas acceptés.*
> - *Il faut se limiter à un seul commentaire par personne.*
> - *Il est interdit de publier plusieurs évaluations dans le but de hausser la réputation ou la note de quelqu'un ou de quelque chose.*
> - *Ne pas inclure des informations personnelles en publiant un commentaire qui pourraient permettre d'identifier l'auteur du commentaire.*

5. Les sites Wikis

Pour minimiser les risques de la navigation sur les sites Wikis, il convient d'adopter une nétiquette qui mentionne les comportements qui ne sont pas tolérables sur le site, ainsi

---

156 Pour voir des exemples de conseils d'écriture qui ont été adoptés : RATEMYPROFESSORS, *Posting Guidelines*, http://www.ratemyprofessors.com/rater_guidelines.jsp; AMAZON, *Conseils d'écriture pour les commentaires d'internautes*, http://www.amazon.fr/gp/customer-reviews/guidelines/review-guidelines.html/171-0464676-0020242 ?ie=UTF8&asin=2266136046; AMAZON, *Review Writing Guidelines*, http://www.amazon.ca/gp/help/customer/display.html/ 701-7159549-0978746 ?ie=UTF8&nodeId=1057790&asin=2266104535; EBAY, *Retrait d'évaluations et évaluations illégales*, http://pages.cafr.ebay.ca/help/policies/feedback-abuse-withdrawal.html.

que les règles de savoir-vivre[157]. Ces règles ont été établies, avec l'usage, par les contributeurs, et en voici des exemples :

> - *Ne pas employer un langage vulgaire, menaçant, diffamant, insultant ou faire des commentaires racistes, à connotation ethnique ou contraire à la loi.*
> - *Les commentaires à caractère pornographique et la publicité ne sont pas acceptés.*
> - *Respecter, en tout temps, le droit d'auteur, et mentionner la source exacte lorsque des citations ou des extraits d'une œuvre sont employés.*
> - *Éviter le plus possible les fautes d'orthographe, en particulier les abréviations utilisées pour d'autres moyens de communication comme le clavardage.*
> - *Éviter de publier des articles de façon anonyme. L'utilisation d'un pseudonyme est acceptée mais il faut fournir une adresse de courriel valide.*
> - *Pour résoudre un conflit qui s'amplifie, il faut essayer de le faire en privé ou sur la page de discussion reliée à l'article en question. Les modifications incessantes de l'article pour effacer le travail de l'autre sont prohibées.*

---

157 Pour voir des exemples de nétiquettes qui ont été adoptées : RS2I.NET, *Netiquette*, http://www.rs2i.net/wiki/Netiquette; WIKIPEDIA, *Wikipedia : Etiquette*, http://en.wikipedia.org/wiki/WP:Wikiquette